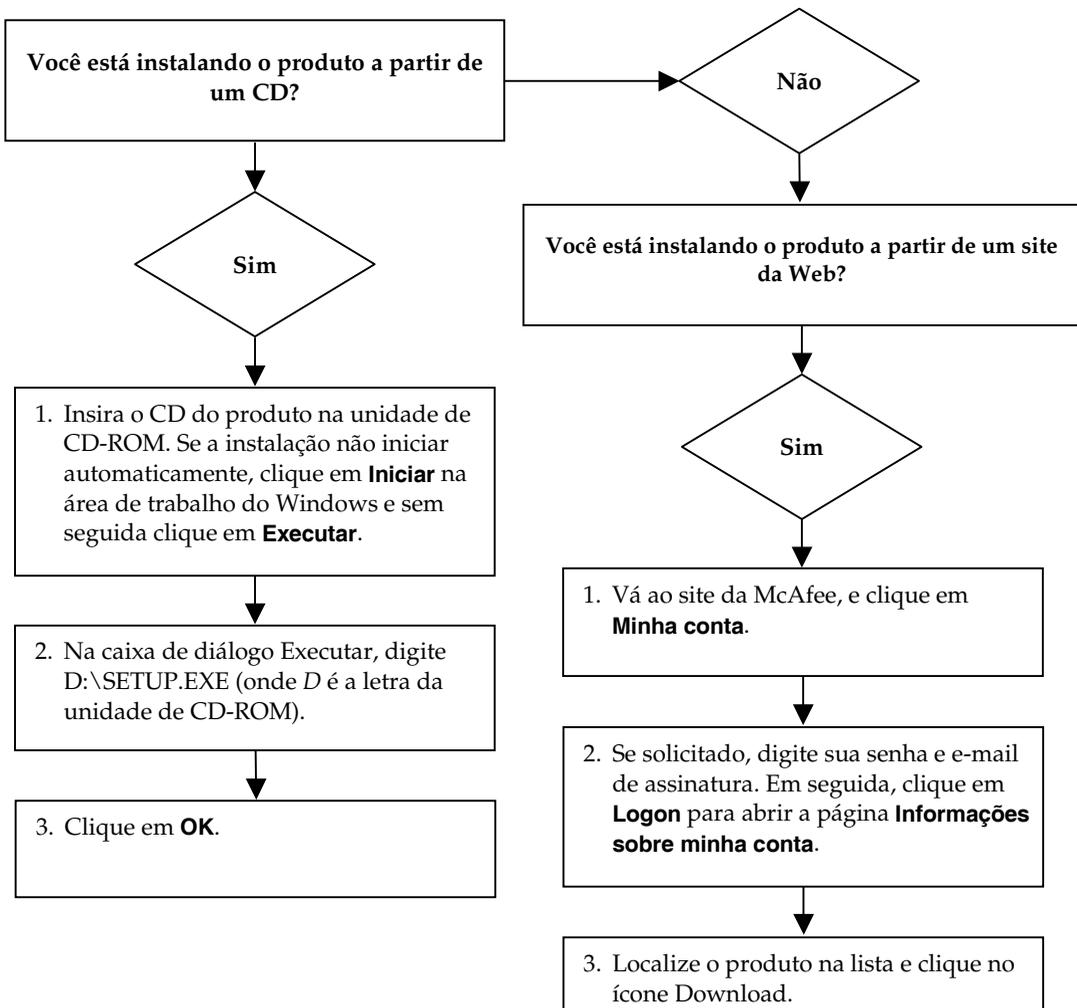
internet**security**suite

Guia do Usuário

Versão 8.0

McAfee®

Cartão de início rápido

Se você estiver instalando o produto de um CD ou de um site da Web, imprima esta página de referência.

Você está instalando o produto a partir de um CD?

Sim

1. Insira o CD do produto na unidade de CD-ROM. Se a instalação não iniciar automaticamente, clique em **Iniciar** na área de trabalho do Windows e sem seguida clique em **Executar**.
2. Na caixa de diálogo Executar, digite D:\SETUP.EXE (onde *D* é a letra da unidade de CD-ROM).
3. Clique em **OK**.

Não

Você está instalando o produto a partir de um site da Web?

Sim

1. Vá ao site da McAfee, e clique em **Minha conta**.
2. Se solicitado, digite sua senha e e-mail de assinatura. Em seguida, clique em **Logon** para abrir a página **Informações sobre minha conta**.
3. Localize o produto na lista e clique no ícone Download.

Para obter mais informações

Para ver os Guias do Usuário contidos no CD do produto, verifique se o Acrobat Reader está instalado. Se não estiver, instale-o agora com o CD do produto da McAfee.

1. Insira o CD do produto na unidade de CD-ROM.
2. Abra o Windows Explorer: Clique em **Iniciar** na área de trabalho do Windows e, em seguida, em **Pesquisar**.
3. Localize a pasta Manuais e clique duas vezes no arquivo.PDF do Guia do Usuário que você deseja abrir.

Benefícios do registro

A McAfee recomenda que você siga as etapas indicadas no produto para que o seu registro seja transmitido diretamente para nós. O registro garante que você receba assistência técnica adequada e confiável, e oferece também os seguintes benefícios:

- Suporte eletrônico GRATUITO.
- Atualizações de arquivos (.DAT) com definição dos vírus por um ano após a instalação quando você adquire o software VirusScan.

  Vá para http://www.mcafee.com/ para obter o preço de um ano adicional das assinaturas de vírus.
- Garantia de 60 dias, que cobre a substituição do CD do software se ele apresentar defeito ou se estiver danificado
- Atualização do filtro SpamKiller por um ano após a instalação quando você adquire o software SpamKiller.

  Vá para http://www.mcafee.com/ para obter o preço de um ano adicional de atualizações do filtro.
- Atualização do pacote McAfee Internet Security por um ano após a instalação quando você adquire o software MIS.

  Vá para http://www.mcafee.com/ para obter o preço de um ano adicional de atualizações do conteúdo.

Suporte técnico

Para obter suporte técnico, consulte

http://www.mcafeehelp.com/.

Nosso site de suporte oferece acesso ininterrupto ao Assistente de Respostas de fácil utilização, que contém soluções para as questões de suporte mais comuns.

Os usuários mais experientes também podem experimentar as opções avançadas, que incluem uma pesquisa de palavra-chave e nossa árvore de ajuda. Se a solução não for encontrada, é possível acessar as opções GRATUITAS do Chat Now! e do E-mail Express!. O Chat e o e-mail ajudam a contatar os engenheiros de suporte qualificados de forma rápida pela Internet, sem custo nenhum. Como alternativa, é possível obter informações do suporte telefônico em

http://www.mcafeehelp.com/.

Conteúdo

Introdução 1

Com um simples clique, você tem acesso a uma vasta gama de informações e opções de entretenimento disponibilizadas pela Internet. No entanto, assim que a conexão é estabelecida, seu computador fica exposto a infindáveis ameaças à privacidade e à segurança. Proteja a privacidade e a segurança de seu computador e de seus dados com o McAfee Internet Security Suite. Incorporando as tecnologias premiadas da McAfee, o Internet Security Suite é um dos conjuntos mais abrangentes de ferramentas de segurança e privacidade disponíveis. O McAfee Internet Security Suite destrói vírus, derrota hackers, protege informações pessoais, privatiza a navegação na Web, bloqueia anúncios e pop-ups, gerencia cookies e senhas, bloqueia arquivos, pastas e unidades, filtra conteúdos censuráveis e permite controlar as conexões de entrada e saída da Internet no computador.

O McAfee Internet Security Suite é uma solução de segurança comprovada, que fornece proteção total aos usuários da Internet de hoje.

O McAfee Internet Security Suite compreende os seguintes produtos:

- *McAfee VirusScan* na página 15
- *McAfee Personal Firewall Plus* na página 49
- *McAfee Privacy Service* na página 81
- *McAfee SpamKiller* na página 99

Software McAfee Internet Security

- **McAfee SecurityCenter —** avalia e informa sobre as vulnerabilidades de segurança de seu computador. Cada índice de segurança avalia rapidamente sua exposição a ameaças de segurança baseadas na Internet e explica como proteger com rapidez e segurança o computador.
- **McAfee VirusScan —** faz a varredura, detecta, corrige e remove vírus da Internet. Você pode personalizar varreduras de vírus e determinar a resposta e a ação quando um vírus é detectado. Também é possível configurar o VirusScan para registrar as ações relacionadas a vírus executadas no seu computador.
- **McAfee Personal Firewall Plus —** protege o computador enquanto ele está conectado à Internet e fornece segurança às conexões de entrada e saída da Internet.
- **McAfee Privacy Service —** combina proteção de informações pessoais (PII), bloqueio de anúncios on-line e filtragem de conteúdo. Esse serviço protege as informações pessoais e proporciona melhor controle do uso da Internet pela sua família. O McAfee Privacy Service garante que as informações confidenciais não fiquem expostas a ameaças on-line e protege você e sua família de conteúdo on-line inadequado.
- **McAfee SpamKiller —** o aumento de e-mails fraudulentos, inadequados e ofensivos enviados a adultos, crianças e empresas torna a proteção contra spam um componente essencial à estratégia de segurança do computador.

Requisitos do sistema

- Microsoft® Windows 98, Me, 2000 ou XP
- Computador com processador compatível com Pentium
  - Windows 98, 2000: 133 MHz ou superior
  - Windows Me: 150 MHz ou superior
  - Windows XP (Home e Pro): 300 MHz ou superior
- RAM
  - Windows 98, Me, 2000: 64 MB
  - Windows XP (Home e Pro): 128 MB
- 100 MB de espaço em disco rígido
- Microsoft® Internet Explorer 5.5 ou posterior

NOTA: Para atualizar para a versão mais recente do Internet Explorer, visite o site da Microsoft em http://www.microsoft.com/.

Usando o McAfee SecurityCenter

O McAfee SecurityCenter é a sua central de produtos de segurança, acessível a partir do ícone correspondente na bandeja de sistema do Windows ou na área de trabalho do Windows. Com ele, você pode executar as seguintes tarefas:

- Obter uma análise gratuita de segurança do seu computador.
- Iniciar, gerenciar e configurar todas as suas assinaturas da McAfee usando um único ícone.
- Exibir alertas de vírus continuamente atualizados e as informações mais recentes sobre os produtos.
- Obter links rápidos para perguntas freqüentes e detalhes da conta no site da McAfee.

> **NOTA**
> Para obter mais informações sobre os recursos do SecurityCenter, clique em **Ajuda** na caixa de diálogo **SecurityCenter**.

Enquanto o SecurityCenter estiver sendo executado e todos os recursos do McAfee instalados no computador estiverem ativados, um ícone com um **M** vermelho será exibido na bandeja de sistema do Windows. Geralmente, essa área se encontra no canto inferior direito da área de trabalho do Windows e contém o relógio.

Se um ou mais aplicativos da McAfee instalados no computador forem desativados, o ícone da McAfee se tornará preto.

Para abrir o McAfee SecurityCenter:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows.
2. Clique em **Abrir o Security Center**.

Para acessar o produto da McAfee:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows.
2. Aponte para o produto da McAfee apropriado e selecione o recurso a ser utilizado.

Removendo programas do Internet Security Suite

Em algumas situações, pode ser necessário remover o Internet Security Suite ou alguns de seus programas.

> **NOTA**
> Para a desinstalação do Internet Security Suite, os usuários devem possuir direitos de administrador.

1. Salve todo o seu trabalho e feche todos os aplicativos abertos.
2. Abra o **Painel de controle**.
   - Na barra de tarefas do Windows, selecione **Iniciar**, aponte para **Configurações** e clique em **Painel de controle** (Windows 98, ME e 2000).
   - Na barra de tarefas do Windows, selecione **Iniciar** e clique em **Painel de controle** (Windows XP).
3. Clique duas vezes em **Adicionar ou remover programas**.
4. Selecione o Assistente de Desinstalação da McAfee, selecione um ou mais programas e clique em **Desinstalar**.
5. Clique em **Sim** para continuar a remoção.
6. Se solicitado, reinicie o computador.

McAfee VirusScan 2

Bem-vindo ao McAfee VirusScan.

O McAfee VirusScan é um serviço de assinatura antivírus que oferece proteção abrangente, confiável e atualizada contra vírus. Equipado com a premiada tecnologia de varredura da McAfee, o VirusScan protege o computador contra vírus, worms, cavalos de Tróia, scripts mal-intencionados e ataques híbridos.

Ele oferece os seguintes recursos:

ActiveShield — faz a varredura dos arquivos quando eles são acessados por você ou pelo seu computador.

Mecanismo de varredura — procura vírus e programas potencialmente indesejados em unidades de disco rígido, disquetes e em arquivos e pastas individuais.

Quarentena — criptografa e isola temporariamente os arquivos infectados e suspeitos na pasta de quarentena até que uma ação apropriada possa ser realizada.

Detecção de atividades hostis — monitora o computador em busca de atividades semelhantes a vírus causadas por scripts mal-intencionados e atividades de worms.

Novos recursos

Esta versão do VirusScan possui os seguintes novos recursos:

- **Detecção e remoção de spyware e adware**
  O VirusScan identifica e remove spyware, adware e outros programas que comprometem a privacidade e reduzem o desempenho do computador.

- **Atualizações automáticas diárias**
  As atualizações automáticas diárias do VirusScan protegem contra as mais recentes ameaças ao computador, identificadas ou não.

- **Varredura rápida em segundo plano**
  Varreduras rápidas e discretas, que identificam e destroem vírus, cavalos de Tróia, worms, spyware, adware, discadores e outros programas mal-intencionado sem interromper o trabalho.

- **Alertas de segurança em tempo real**
  Os alertas de segurança notificam sobre epidemias de vírus de emergência e ameaças à segurança. Também oferecem opções de resposta para remover, neutralizar ou aprender mais sobre a ameaça.

- **Detecção e limpeza em vários pontos de entrada**
  O VirusScan monitora e limpa os principais pontos de entrada do computador: e-mails, anexos de mensagens instantâneas e downloads da Internet.

- **Monitoração de atividades semelhantes às de worms em e-mails**
  O WormStopper™ monitora comportamentos suspeitos de envio de mensagens em massa e impede a disseminação de vírus e worms por e-mail em outros computadores.

- **Monitoração de atividades semelhantes às de worms em scripts**
  O ScriptStopper™ monitora a execução de scripts suspeitos e impede a disseminação de vírus e worms por e-mail em outros computadores.

- **Suporte técnico gratuito por e-mail e mensagens instantâneas**
  O suporte técnico ao vivo fornece assistência imediata e fácil, usando troca de mensagens instantâneas e e-mails.

Testando o VirusScan

Antes de começar a usar o VirusScan, deve-se testar a sua instalação. Use as etapas a seguir para testar separadamente os recursos Fazer varredura e ActiveShield.

Testando o ActiveShield

NOTA
Para testar o ActiveShield na guia VirusScan do SecurityCenter, clique em **Testar VirusScan** para exibir a seção de FAQ do suporte online que contém as etapas a serem executadas.

Para testar o ActiveShield:

1 Vá para http://www.eicar.com/ no seu navegador da web.

2 Clique no link **The AntiVirus testfile eicar.com**.

3 Vá para o final da página. Em **Download**, você verá quatro links.

4 Clique em **eicar.com**.

Se o ActiveShield estiver funcionando adequadamente, ele detectará o arquivo eicar.com imediatamente após o clique no link. Experimente excluir ou colocar em quarentena arquivos infectados para saber como o ActiveShield lida com os vírus. Consulte *Entendendo os alertas de segurança* na página 30 para obter detalhes.

Testando a varredura

Antes de testar o mecanismo de varredura, é necessário desativar o ActiveShield para impedir que ele detecte os arquivos infectados antes da varredura. Após desativá-lo, faça o download dos arquivos de teste.

Para fazer download de arquivos de teste:

1. Desative o ActiveShield: Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Desativar**.
2. Faça o download de arquivos de teste EICAR no site da EICAR:
   a. Vá para http://www.eicar.com/.
   b. Clique no link **The AntiVirus testfile eicar.com**.
   c. Vá para o final da página. Em **Download**, você verá estes links:

      O arquivo **eicar.com** contém uma linha de texto que o VirusScan detecta como vírus.

      O arquivo **eicar.com.txt** (opcional) é o mesmo arquivo, mas com outro nome, para usuários com dificuldade em fazer o download no primeiro link. Simplesmente renomeie o arquivo como “eicar.com” após o download.

      O arquivo **eicar_com.zip** é uma cópia do vírus de teste, em um arquivo compactado .ZIP (arquivo WinZip™).

      O arquivo **eicarcom2.zip** é uma cópia do vírus de teste em um arquivo compactado .ZIP que, por sua vez, encontra-se em um arquivo compactado .ZIP.

   d. Clique em cada link para fazer o download do arquivo correspondente. Para cada arquivo, é exibida uma caixa de diálogo **Download de arquivo**.
   e. Clique em **Salvar**, clique no botão **Criar nova pasta** e renomeie a pasta como **Pasta de varredura de VSO**.
   f. Clique duas vezes em **Pasta de varredura de VSO** e, em seguida, clique em **Salvar** novamente, em todas as caixas de diálogo **Salvar como**.
3. Quando terminar o download dos arquivos, feche o Internet Explorer.
4. Ative o ActiveShield: Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Ativar**.

Para testar a opção Fazer varredura:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Fazer varredura**.
2. Utilizando a árvore de diretório no painel esquerdo da caixa de diálogo, vá até a **Pasta de varredura de VSO** em que você salvou os arquivos:
   a. Clique no sinal **+** ao lado do ícone da unidade C.
   b. Clique em **Pasta de varredura de VSO** para selecioná-la (não clique no sinal **+** ao lado dessa opção).

      Isso indica que a opção Fazer varredura deve verificar se há vírus apenas nessa pasta. Você também pode colocar os arquivos em locais aleatórios na unidade de disco rígido para obter uma demonstração mais convincente da capacidade do recurso Fazer varredura.
3. Na área **Opções de varredura** da caixa de diálogo **Fazer varredura**, verifique se todas as opções estão selecionadas.
4. Clique em **Fazer varredura** na parte inferior direita da caixa de diálogo.

   O VirusScan examina a **Pasta de varredura de VSO**. Os arquivos de teste EICAR salvos nessa pasta são exibidos na **Lista de arquivos detectados**. Se isso ocorrer, a varredura estará funcionando adequadamente.

Experimente excluir ou colocar em quarentena os arquivos infectados para saber como o recurso Fazer varredura lida com vírus. Consulte *Entendendo as detecções de ameaças* na página 39 para obter detalhes.

Usando o ActiveShield

Quando iniciado (carregado na memória do computador) e ativado, o ActiveShield passa a proteger continuamente o computador. O ActiveShield faz a varredura dos arquivos quando eles são acessados por você ou pelo computador. Quando detecta um arquivo infectado, o ActiveShield tenta limpar automaticamente o vírus. Se o ActiveShield não puder limpar o vírus, coloque o arquivo em quarentena ou exclua-o.

Ativando ou desativando o ActiveShield

Por padrão, o ActiveShield é iniciado (carregado na memória do computador) e ativado (representado pelo M vermelho na bandeja de sistema do Windows) assim que o computador é reiniciado após o processo de instalação.

Se o ActiveShield for interrompido (não carregado) ou desativado (indicado pelo ícone em preto M), você poderá executá-lo manualmente e configurá-lo para iniciar automaticamente com o Windows.

Ativando o ActiveShield

Para ativar o ActiveShield somente nesta sessão do Windows:

Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Ativar**. A cor do ícone da McAfee muda para vermelho .

Se o ActiveShield ainda estiver configurado para iniciar com o Windows, uma mensagem informará que você está protegido contra vírus. Caso contrário, será exibida uma caixa de diálogo em que você poderá configurar o ActiveShield para ser iniciado com o Windows (Figura 2-1 na página 20).

Desativando o ActiveShield

Para desativar o ActiveShield somente nesta sessão do Windows:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Desativar**.

2 Clique em **Sim** para confirmar.

   A cor do ícone da McAfee muda para preto .

Se o ActiveShield ainda estiver configurado para iniciar com o Windows, o computador estará protegido contra vírus novamente quando você o reiniciar.

Configurando as opções do ActiveShield

É possível modificar as opções de inicialização e varredura da guia **ActiveShield** na caixa de diálogo **Opções do VirusScan** (Figura 2-1), acessível por meio do ícone da McAfee na bandeja de sistema do Windows.

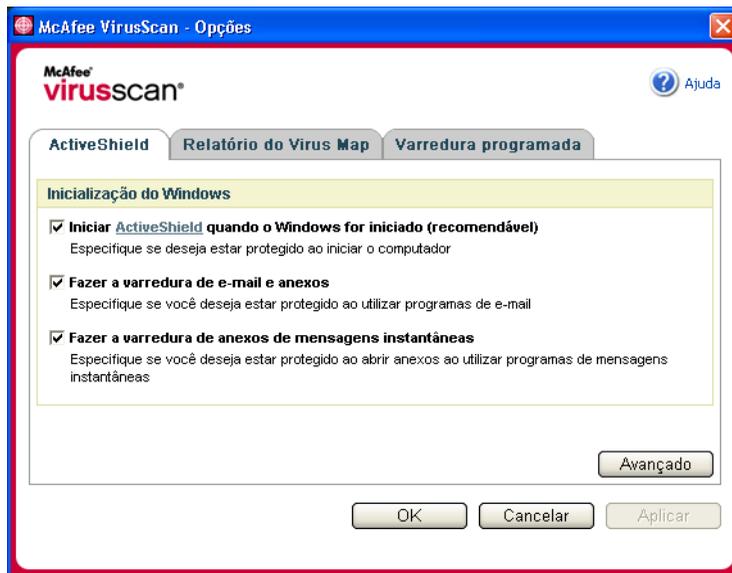



Figura 2-1. Opções do ActiveShield

Iniciando o ActiveShield

Por padrão, o ActiveShield é iniciado (carregado na memória do computador) e ativado (representado por vermelho) assim que o computador é reiniciado após o processo de instalação.

Se o ActiveShield for interrompido (representado por preto), você poderá configurá-lo para iniciar automaticamente com o Windows (recomendável).

NOTA

Durante as atualizações do VirusScan, o **Assistente de atualização** pode interromper o ActiveShield temporariamente para instalar arquivos novos. Quando o **Assistente de atualização** solicitar que você clique em **Concluir**, o ActiveShield será iniciado novamente.

Para iniciar o ActiveShield automaticamente com o Windows :

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.

   A caixa de diálogo **Opções do VirusScan** será aberta (Figura 2-1 na página 20).

2 Marque a caixa de seleção **Iniciar o ActiveShield quando o Windows for iniciado (recomendável)** e clique em **Aplicar** para salvar as alterações.

3 Clique em **OK** para confirmar e, em seguida, clique em **OK**.

Interrompendo o ActiveShield

AVISO
Se você interromper o ActiveShield, o seu computador não estará protegido contra vírus. Se for necessário interromper o ActiveShield para outros fins que não seja a atualização do VirusScan, certifique-se de não estar conectado à Internet.

Para não iniciar o ActiveShield com o Windows:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.

   A caixa de diálogo **Opções do VirusScan** será aberta (Figura 2-1 na página 20).

2 Desmarque a caixa de seleção **Iniciar o ActiveShield quando o Windows for iniciado (recomendável)** e clique em **Aplicar** para salvar as alterações.

3 Clique em **OK** para confirmar e, em seguida, clique em **OK**.

Fazendo a varredura de e-mails e anexos

Por padrão, a varredura de e-mails e a limpeza automática são ativadas com a opção **Fazer a varredura de e-mail e anexos** (Figura 2-1 na página 20).

Quando essa opção está ativada, o ActiveShield faz a varredura automaticamente e tenta limpar as mensagens e os anexos de e-mail infectados enviados (SMTP) e recebidos (POP3) pelos clientes de e-mail mais utilizados, incluindo os seguintes:

- Microsoft Outlook Express 4.0 ou posterior
- Microsoft Outlook 97 ou posterior
- Netscape Messenger 4.0 ou posterior
- Netscape Mail 6.0 ou posterior
- Eudora Light 3.0 ou posterior
- Eudora Pro 4.0 ou posterior
- Eudora 5.0 ou posterior
- Pegasus 4.0 ou posterior

NOTA
Não há suporte à varredura de e-mails nos seguintes clientes de e-mail: clientes baseados na Web, IMAP, AOL, POP3 SSL e Lotus Notes. No entanto, o ActiveShield faz a varredura de anexos de e-mail quando são abertos.

Quando a opção **Fazer a varredura de e-mail e anexos** é desativada, as opções de varredura de e-mails e do WormStopper (Figura 2-2 na página 23) são desativadas automaticamente. Quando a varredura de e-mails enviados é desativada, as opções do WormStopper são desativadas automaticamente.

Se você alterar as opções de varredura de e-mails, reinicie o programa de e-mail para efetuar essas alterações.

E-mails recebidos

Quando uma mensagem ou um anexo de e-mail recebido está infectado, o ActiveShield executa as seguintes etapas:

- Tenta limpar o e-mail infectado.
- Tenta colocar em quarentena ou excluir o e-mail que não pode ser limpo.
- Inclui um arquivo de alerta no e-mail recebido, contendo informações sobre as ações a serem executadas para remover a infecção.

E-mails enviados

Quando uma mensagem ou um anexo de e-mail enviado está infectado, o ActiveShield executa as seguintes etapas:

- Tenta limpar o e-mail infectado.
- Tenta colocar em quarentena ou excluir o e-mail que não pode ser limpo.

NOTA
Para obter detalhes sobre os erros da varredura de e-mails enviados, consulte a ajuda online.

Desativando a varredura de e-mails

Por padrão, o ActiveShield faz a varredura de e-mails recebidos e enviados. Porém, para melhor controle, é possível configurar o ActiveShield para fazer a varredura somente de e-mails recebidos ou enviados.

Para desativar a varredura de e-mails recebidos ou enviados:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.
2. Clique em **Avançado** e, em seguida, clique na guia **Varredura de e-mail** (Figura 2-2).

3 Desmarque **Mensagens de e-mail recebidas** ou **Mensagens de e-mail enviadas** e clique em **OK**.

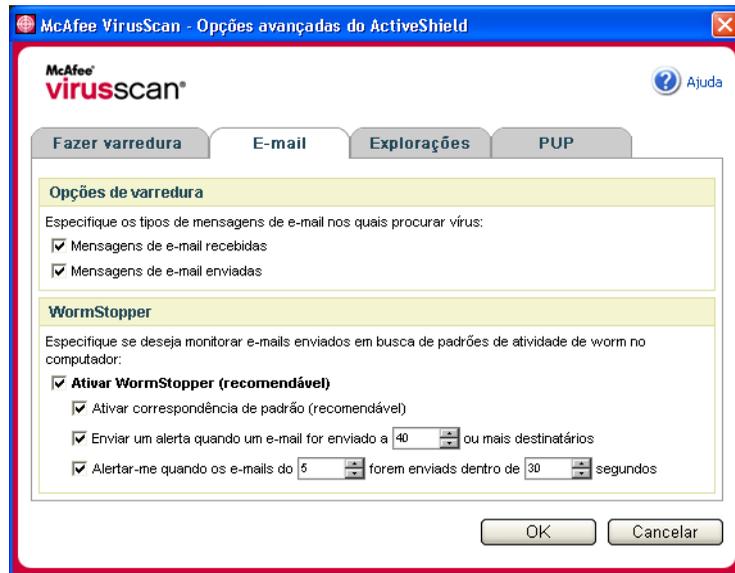



Figura 2-2. Opções avançadas do ActiveShield - guia E-mail

Fazendo a varredura de worms

O VirusScan monitora o computador verificando atividades suspeitas que podem indicar a presença de ameaças. Enquanto o VirusScan limpa vírus, o WormStopper™ evita a disseminação posterior de vírus e worms.

Um “worm“ de computador é um vírus que se replica automaticamente, reside na memória e pode enviar cópias de si mesmo por e-mail. Sem o WormStopper, os worms são percebidos apenas quando suas réplicas descontroladas consomem recursos do sistema, diminuindo o desempenho ou interrompendo tarefas.

O mecanismo de proteção do WormStopper detecta, alerta e bloqueia atividades mal-intencionadas. As atividades suspeitas podem executar as seguintes ações no computador:

- Tentativas de encaminhar e-mails a muitos contatos da lista de endereços.
- Tentativas de encaminhar várias mensagens de e-mail em uma seqüência rápida

Quando o ActiveShield está configurado para usar a opção padrão **Ativar WormStopper (recomendável)** da caixa de diálogo **Opções avançadas**, o WormStopper monitora a atividade de e-mail em busca de padrões de atividades suspeitas e envia alertas quando o número especificado de e-mails ou destinatários é excedido em um determinado intervalo.

Para configurar o ActiveShield para fazer a varredura de mensagens de e-mail enviadas quanto a atividades semelhantes a worms:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.

2 Clique em **Avançado** e, em seguida, clique na guia **E-mail**.

3 Clique em **Ativar WormStopper (recomendável)** (Figura 2-3).

Por padrão, as seguintes opções detalhadas estão ativadas:

- Correspondência de padrões para detectar atividades suspeitas
- Envio de alertas quando um e-mail é enviado a 40 ou mais destinatários
- Envio de alertas quando 5 ou mais e-mails são enviados em 30 segundos

NOTA
Se você alterar o número de destinatários ou de segundos para a monitoração de e-mails enviados, poderão ocorrer detecções inválidas. A McAfee recomenda clicar em **Não** para manter as configurações padrão. Se preferir, clique em **Sim** para alterar as configurações padrão.

Essa opção pode ser ativada automaticamente após a detecção de um possível worm pela primeira vez (consulte detalhes em *Gerenciando possíveis worms* na página 31):

- Bloqueio automático de e-mails suspeitos enviados

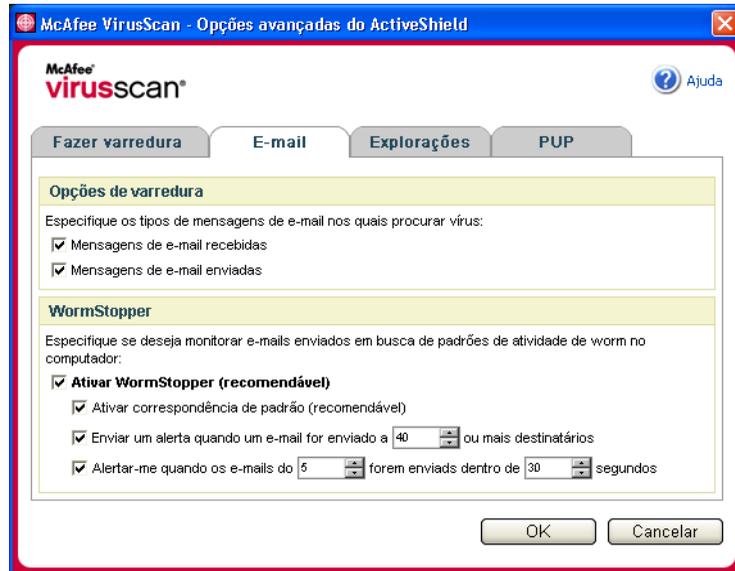



Figura 2-3. Opções avançadas do ActiveShield - guia E-mail

Fazendo a varredura de anexos de mensagens instantâneas recebidas

Por padrão, a varredura de anexos de mensagens instantâneas é ativada com a opção **Fazer a varredura de anexos de mensagens instantâneas**. (Figura 2-1 na página 20).

Quando essa opção está ativada, o VirusScan faz a varredura automática e tenta limpar os anexos infectados de mensagens instantâneas recebidas dos programas de mensagens instantâneas mais utilizados, incluindo os seguintes:

- MSN Messenger 6.0 ou posterior
- Yahoo Messenger 4.1 ou posterior
- AOL Instant Messenger 2.1 ou posterior

NOTA
Para sua proteção, não é possível desativar a limpeza automática dos anexos de mensagens instantâneas.

Quando um anexo de mensagem instantânea recebida está infectado, o VirusScan executa as seguintes etapas:

- Tenta limpar a mensagem infectada
- Pergunta se deve colocar em quarentena ou excluir a mensagem que não pode ser limpa

Fazendo a varredura de todos os arquivos

Quando o ActiveShield é configurado para usar a opção padrão **Todos os arquivos (recomendável)**, ele faz a varredura de todos os tipos de arquivos existentes no computador à medida que este tenta utilizá-los. Utilize esta opção para obter a varredura mais completa possível.

Para configurar o ActiveShield para fazer a varredura de todos os tipos de arquivos:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.
2. Clique em **Avançado** e, em seguida, clique na guia **Varredura** (Figura 2-4 na página 26).
3. Clique em **Todos os arquivos (recomendável)** e, em seguida, clique em **OK**.

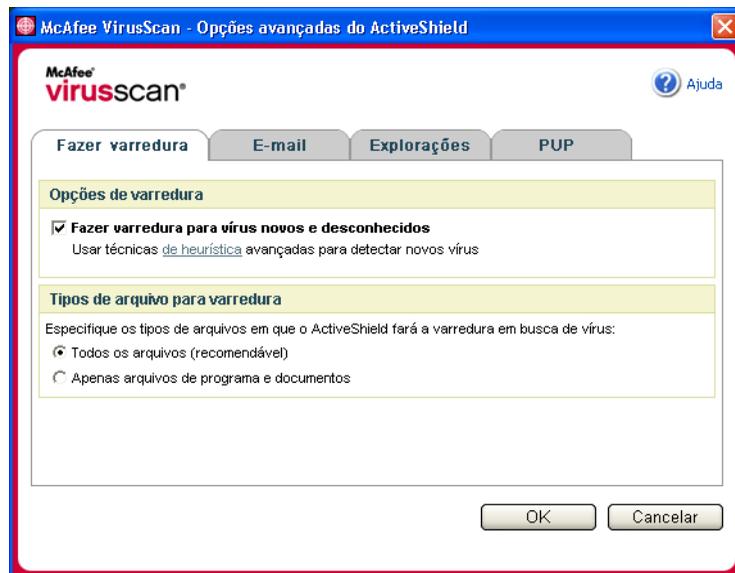



Figura 2-4. Opções avançadas do ActiveShield - guia Fazer varredura

Fazendo a varredura somente de arquivos de programas e documentos

Quando o ActiveShield é configurado para usar a opção **Apenas arquivos de programa e documentos**, ele realiza a varredura somente de documentos e arquivos de programas. O arquivo de assinatura de vírus mais recente (arquivo DAT) determina os tipos de arquivos a serem examinados pelo ActiveShield. Para configurar o ActiveShield para fazer a varredura apenas de arquivos de programas e documentos:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.
2. Clique em **Avançado** e, em seguida, clique na guia **Fazer varredura**. (Figura 2-4).
3. Clique em **Apenas arquivos de programa e documentos** e, em seguida, clique em **OK**.

Fazendo a varredura em busca de vírus novos e desconhecidos

Quando o ActiveShield é configurado para usar a opção padrão **Fazer varredura para vírus novos e desconhecidos (recomendável)**, ele utiliza técnicas heurísticas avançadas que tentam estabelecer uma correspondência entre os arquivos e as assinaturas de vírus conhecidos. Ao mesmo tempo, procura indícios de vírus desconhecidos nos arquivos..

Para configurar o ActiveShield para fazer a varredura de vírus novos e desconhecidos:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.
2. Clique em **Avançado** e, em seguida, clique na guia **Fazer varredura**. (Figura 2-4).
3. Clique em **Fazer a varredura para vírus novos e desconhecidos (recomendável)** e, em seguida, clique em **OK**.

Fazendo a varredura de scripts

O VirusScan monitora o computador verificando atividades suspeitas que podem indicar a presença de ameaças. Enquanto o VirusScan limpa vírus, o ScriptStopper™ evita que cavalos de Tróia executem os scripts que disseminam ainda mais os vírus.

Um “cavalo de Tróia” é um programa mal-intencionado que finge ser um aplicativo benigno. Eles não são vírus porque não se replicam, mas podem ser tão destruidores quanto os vírus.

O mecanismo de proteção do ScriptStopper detecta, alerta e bloqueia atividades mal-intencionadas. As atividades suspeitas podem executar a seguinte ação em seu computador:

- Execução de scripts que resultam na criação, cópia ou exclusão de arquivos ou na abertura do Registro do Windows.

Quando o ActiveShield é configurado para usar a opção padrão **Ativar ScriptStopper (recomendável)** caixa de diálogo de **Opções avançadas**, o ScriptStopper monitora a execução de scripts e a atividade de e-mail em busca de padrões de atividades suspeitas e envia alertas quando o número especificado de e-mails ou destinatários excede um determinado intervalo.

Para configurar o ActiveShield para fazer a varredura de scripts em execução cuja atividade seja semelhante à de worms:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.
2. Clique em **Avançado** e, em seguida, clique na guia **Explorações** (Figura 2-5).
3. Clique em **Ativar ScriptStopper (recomendável)** e, em seguida, clique em **OK**.

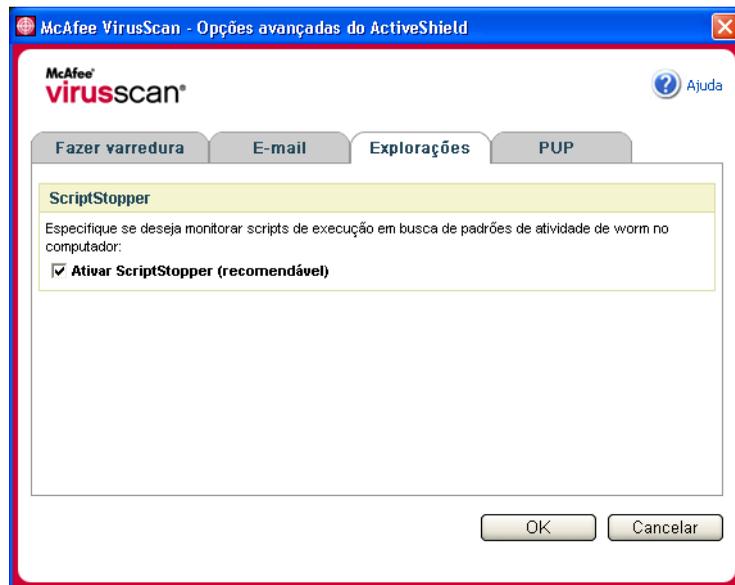



Figura 2-5. Opções avançadas do ActiveShield - guia Explorações

Fazendo a varredura de programas potencialmente indesejados (PUPs)

NOTA
Após ser instalado no computador, o McAfee AntiSpyware gerencia todas as atividades de programas potencialmente indesejados (PUPs). Abra o McAfee AntiSpyware para configurar as opções.

Quando o ActiveShield é configurado para usar a opção padrão **Fazer a varredura de programas potencialmente indesejados (recomendado)** na caixa de diálogo **Opções Avançadas**, a proteção contra programas potencialmente indesejados (PUPs) detecta, bloqueia e remove rapidamente spywares, adwares e outros malwares que coletam e transmitem dados particulares sem permissão.

Para configurar o ActiveShield para fazer a varredura de PUPs:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.

2 Clique em **Avançado** e, em seguida, clique na guia **PUPs** (Figura 2-6).

3 Clique em **Fazer a varredura de programas potencialmente indesejados (recomendável)** e, em seguida, clique em **OK**.

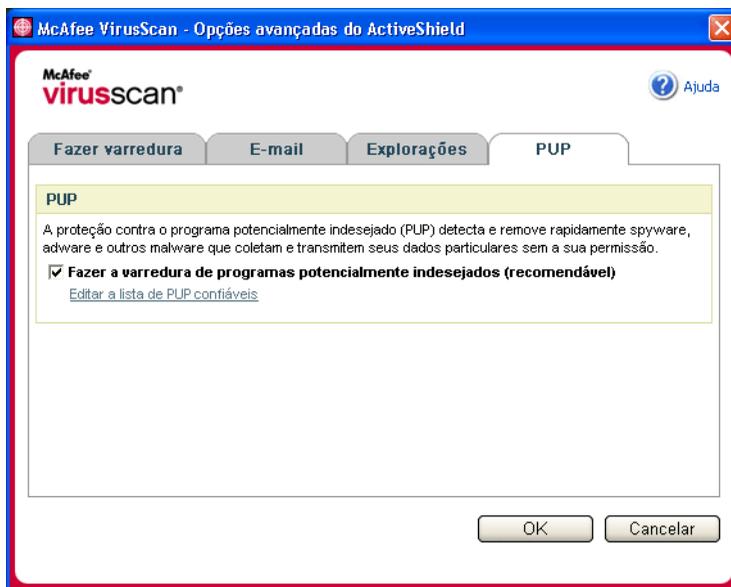



Figura 2-6. Opções avançadas do ActiveShield - guia PUPs

Entendendo os alertas de segurança

Quando o ActiveShield detecta um vírus, é exibido um alerta semelhante a Figura 2-7. Para a maioria dos vírus, cavalos de Tróia, e worms, o ActiveShield tenta limpar automaticamente o arquivo e envia um alerta a você. Para programas potencialmente indesejados (PUPs), o ActiveShield detecta o arquivo, bloqueia-o automaticamente e envia um alerta a você.

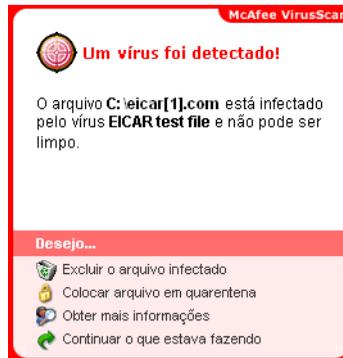



Figura 2-7. Alerta de vírus

Você pode escolher como gerenciar arquivos infectados, e-mails infectados, scripts suspeitos, worms potenciais ou PUPs e se deseja enviar os arquivos infectados aos laboratórios AVERT da McAfee para que sejam pesquisados.

Para maior proteção, sempre que o ActiveShield detecta um arquivo suspeito, é solicitada a realização imediata de uma varredura em todo o computador. A menos que escolha ocultar o aviso da varredura, você receberá lembretes periódicos até executá-la.

Gerenciando arquivos infectados

1 Se o ActiveShield puder limpar o arquivo, você poderá obter mais informações ou ignorar o alerta:

   - Clique em **Obter mais informações** para exibir o nome, o local e o nome do vírus associado ao arquivo infectado.

   - Clique em **Continuar o que eu estava fazendo** para ignorar o alerta e fechá-lo.

2 Se o ActiveShield não puder limpar o arquivo, clique em **Colocar o arquivo em quarentena** para criptografar e isolar temporariamente arquivos infectados e suspeitos no diretório de quarentena até que uma ação adequada possa ser executada.

Uma mensagem de confirmação é exibida, solicitando que seja verificada a existência de vírus no computador. Clique em **Fazer varredura** para concluir o processo de quarentena.

3 Se o ActiveShield não puder colocar o arquivo em quarentena, clique em **Excluir o arquivo infectado** para tentar remover o arquivo.

Gerenciando e-mails infectados

Por padrão, a varredura de e-mails tenta limpar automaticamente o e-mail infectado. Um arquivo de alerta incluído na mensagem de saída informa se o e-mail foi limpo, colocado em quarentena ou excluído.

Gerenciando scripts suspeitos

Quando o ActiveShield detecta um script suspeito, você pode obter mais informações e interromper o script, caso não tenha pretendido iniciá-lo:

- Clique em **Obter mais informações** para exibir o nome, o local e a descrição da atividade associada ao script suspeito.
- Clique em **Interromper este script** para impedir a execução de scripts suspeitos.

Se tiver certeza de que o script é confiável, você pode permitir que ele seja executado:

- Clique em **Permitir este script desta vez** para permitir a execução de todos os scripts contidos em um único arquivo uma vez.
- Clique em **Continuar o que estava fazendo** para ignorar o alerta e deixar o script ser executado.

Gerenciando possíveis worms

Quando o ActiveShield detecta um possível worm, você pode obter mais informações e interromper a atividade de e-mail, caso não tenha pretendido iniciá-la:

- Clique em **Obter mais informações** para exibir a lista de destinatários, a linha de assunto, o corpo da mensagem e uma descrição da atividade suspeita associada à mensagem de e-mail infectada.
- Clique em **Interromper este e-mail** para impedir o envio do e-mail e excluí-lo da fila de mensagens.

Se tiver certeza de que o e-mail é confiável, clique em **Continuar o que estava fazendo** para ignorar o alerta e permitir o envio do e-mail.

Gerenciando PUPs

Se o ActiveShield detectar e bloquear um programa potencialmente indesejado (PUP), você poderá obter mais informações e remover o programa, caso não pretenda instalá-lo:

- Clique em **Obter mais informações** para exibir o nome, o local e a ação recomendada associada ao PUP.
- Clique em **Remover este PUP** para remover o programa, caso não pretenda instalá-lo.

  Uma mensagem de confirmação é exibida.

  - Se (a) você não reconhecer o PUP ou (b) não tiver instalado o PUP como parte de um pacote ou aceitado um acordo de licença de fornecedor associado a esses programas, clique em **OK** para remover o programa usando o método da McAfee.

  - Caso contrário, clique em **Cancelar** para sair do processo de remoção automática. Caso mude de idéia posteriormente, poderá remover o programa manualmente, usando o programa de desinstalação do fornecedor.
- Clique em **Continuar o que estava fazendo** para ignorar o alerta e bloquear o programa desta vez.

Se você (a) reconhecer o PUP ou (b) tiver instalado o PUP como parte de um pacote ou aceitado um acordo de licença de fornecedor associado a esses programas, poderá permitir sua execução:

- Clique em **Confiar neste PUP** para incluir o programa na lista branca e sempre permitir sua execução no futuro.

  Consulte "*Gerenciando PUPs confiáveis*" para obter detalhes.

Gerenciando PUPs confiáveis

Os programas adicionados à lista de PUPs confiáveis não são detectados pelo McAfee VirusScan.

Se um PUP for detectado e adicionado à lista de PUPs confiáveis, ele poderá ser removido posteriormente, se necessário.

Se a lista de PUPs estiver cheia, será necessário remover alguns itens da lista para poder confiar em outro PUP.

Para remover um programa da lista de PUPs confiáveis:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.
2. Clique em **Avançado** e, em seguida, clique na guia **PUPs**.
3. Clique em **Editar lista de PUPs confiáveis**, marque a caixa de seleção ao lado do nome do arquivo e clique em **Remover**. Clique em **OK** quando terminar de remover os itens.

Fazendo a varredura manual do computador

O mecanismo de varredura permite procurar vírus e programas potencialmente indesejados (PUP) em unidades de disco rígido, disquetes e em arquivos e pastas individuais. Ao encontrar um arquivo infectado, o mecanismo tenta limpá-lo automaticamente, a não ser que seja um programa potencialmente indesejado. Se o mecanismo de varredura não conseguir limpar o vírus, você poderá colocar o arquivo em quarentena ou excluí-lo.

Fazendo a varredura manual de vírus e outras ameaças

Para fazer a varredura do computador:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Fazer varredura**.

   A caixa de diálogo **Fazer varredura** será aberta (Figura 2-8).

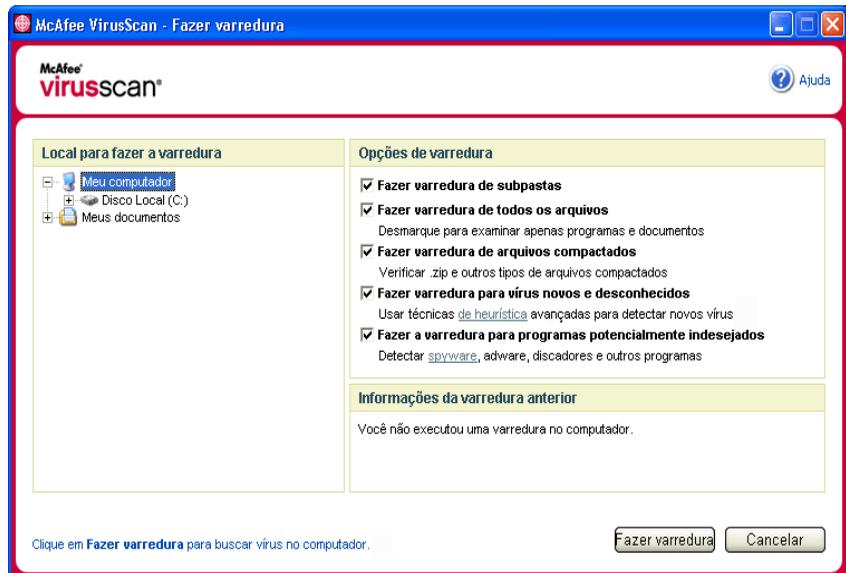



Figura 2-8. Caixa de diálogo Fazer varredura

2 Clique na unidade, pasta ou arquivo em que será feita a varredura.

3 Selecione as **Opções de varredura**. Por padrão, todas as **Opções de varredura** padrão são previamente selecionadas para oferecer a varredura mais completa possível (Figura 2-8):

- **Fazer varredura de subpastas** — use essa opção para fazer a varredura de arquivos contidos nas suas subpastas. Desmarque essa caixa de seleção para permitir a verificação somente dos arquivos que podem ser vistos quando uma pasta ou uma unidade é aberta.

  Exemplo: Os arquivos da Figura 2-9 serão os únicos examinados, se você desmarcar a caixa **Fazer varredura de subpastas**. As pastas e seu conteúdo não serão examinados. Para examinar as pastas e seu conteúdo, é necessário deixar marcada essa caixa de seleção.

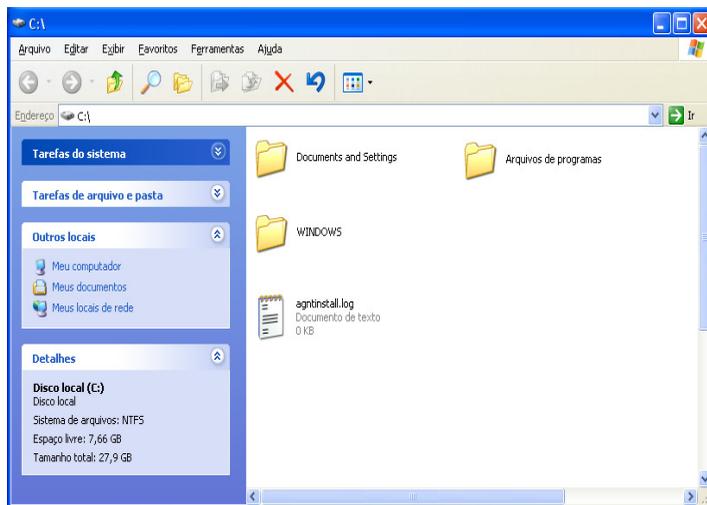



Figura 2-9. Conteúdo do disco local

- **Fazer varredura de todos os arquivos** — use essa opção para permitir a varredura completa de todos os arquivos. Desmarque essa caixa de seleção para diminuir o tempo da varredura e permitir a verificação apenas de documentos e arquivos de programas.

- **Fazer varredura de arquivos compactados** — use essa opção para revelar arquivos infectados ocultos em arquivos .ZIP e outros arquivos compactados. Desmarque essa caixa de seleção para evitar a varredura de arquivos ou arquivos compactados que se encontram em outros arquivos compactados.

  Às vezes, os autores inserem vírus em arquivos .ZIP, inserem esses arquivos .ZIP em outros arquivos .ZIP, visando a burlar os mecanismos antivírus. O mecanismo de varredura pode detectar esses vírus desde que essa opção esteja selecionada.

- **Fazer varredura para vírus novos e desconhecidos** — use essa opção para encontrar os vírus mais recentes para os quais talvez não existam "vacinas". A opção utiliza técnicas heurísticas avançadas que tentam estabelecer uma correspondência dos arquivos às assinaturas de vírus conhecidos. Ao mesmo tempo, são procurados indícios de vírus desconhecidos nos arquivos.

  Esse método de varredura também examina o arquivo em busca de características que geralmente indicam que ele contém vírus. Isso minimiza a possibilidade de a varredura fornecer indicações falsas. Porém, se uma varredura heurística detectar um vírus, trate-o com o mesmo cuidado destinado a arquivos que você sabe que contêm vírus.

  Essa opção proporciona a varredura mais completa, mas geralmente é mais lenta do que a varredura normal.

- **Fazer a varredura para programas potencialmente indesejados** — use essa opção para detectar spywares, adwares, discadores e outros programas potencialmente indesejados.

  NOTA
  Mantenha todas as opções padrão selecionadas para obter a varredura mais completa possível. Esse procedimento fará a varredura de todos os arquivos da unidade ou da pasta selecionada. Portanto, reserve tempo suficiente para que a varredura seja concluída. Quanto maior a unidade de disco rígido e o número de arquivos existentes, mais demorada será a varredura.

4 Clique em **Fazer varredura** para iniciar a varredura de arquivos.

Quando a varredura for concluída, um resumo informará o número de arquivos examinados e de arquivos detectados, além do número de programas potencialmente indesejados e arquivos detectados que foram limpos automaticamente.

5 Clique em **OK** para fechar o resumo e exibir a lista de todos os arquivos detectados na caixa de diálogo **Fazer varredura** (Figura 2-10).

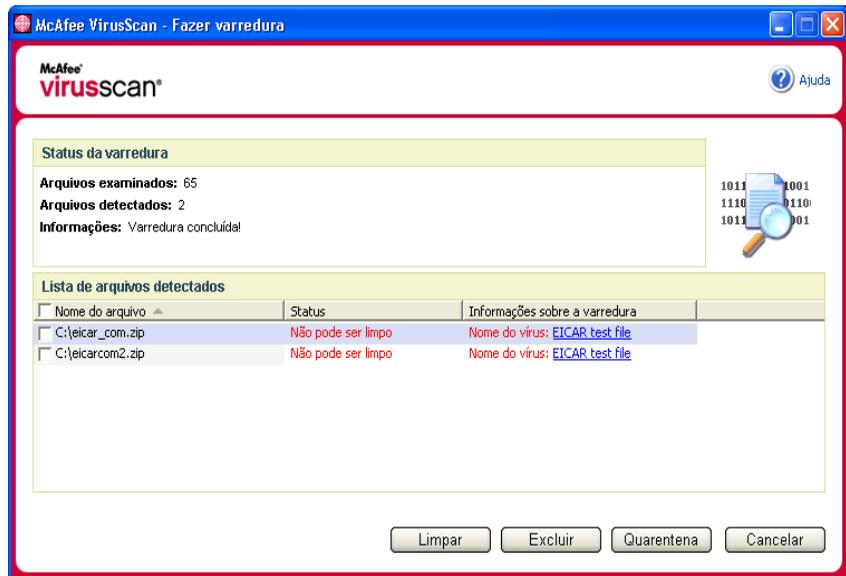



Figura 2-10. Resultados da varredura

NOTA
A varredura considera um arquivo compactado (.ZIP, .CAB, etc.) como um arquivo único na contagem dos **Arquivos examinados**. Além disso, o número de arquivos examinados pode variar se você tiver excluído os arquivos temporários da Internet após a última varredura.

6 Se o mecanismo de varredura não encontrar vírus ou programas potencialmente indesejados, clique em **Voltar** para selecionar outra pasta ou unidade para a varredura ou clique em **Fechar** para fechar a caixa de diálogo. Caso contrário, consulte *Entendendo as detecções de ameaças* na página 39.

Fazendo a varredura pelo Windows Explorer

O VirusScan fornece um menu de atalho que permite fazer a varredura de arquivos, pastas ou unidades a partir do Windows Explorer em busca de vírus e programas potencialmente indesejados.

Para fazer a varredura de arquivos no Windows Explorer:

1 Abra o Windows Explorer.

2 Clique com o botão direito do mouse na unidade, pasta ou arquivo em que a varredura será realizada e clique em **Fazer varredura**.

   A caixa de diálogo **Fazer varredura** será aberta e iniciará a varredura dos arquivos. Todas as **Opções de varredura** padrão são previamente selecionadas para oferecer a varredura mais completa possível (Figura 2-8 na página 33).

Fazendo a varredura pelo Microsoft Outlook

O VirusScan fornece um ícone de barra de ferramentas para o Microsoft Outlook 97 ou posterior, que permite verificar a existência de vírus ou programas potencialmente indesejados nos locais selecionados de armazenamento de mensagens e respectivas subpastas, pastas de caixa de correio ou mensagens de e-mail com anexos.

Para fazer a varredura de e-mails no Microsoft Outlook:

1 Abra o Microsoft Outlook.

2 Clique no local de armazenamento de mensagens, pasta ou mensagem de e-mail que contém o anexo a ser examinado e clique no ícone de varredura de e-mails da barra de ferramentas .

   O mecanismo de varredura de e-mails é aberto e inicia a varredura dos arquivos. Todas as **Opções de varredura** padrão são previamente selecionadas para oferecer a varredura mais completa possível (Figura 2-8 na página 33).

Fazendo a varredura automática de vírus e outras ameaças

Embora o VirusScan faça a varredura de arquivos à medida que são acessados por você ou pelo computador, é possível programar a varredura automática no Agendador do Windows para procurar minuciosamente vírus e programas potencialmente indesejados no computador em intervalos especificados.

Para programar uma varredura:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.

   A caixa de diálogo **Opções do VirusScan** será aberta.

2 Clique na guia **Varredura programada** (Figura 2-11 na página 38).

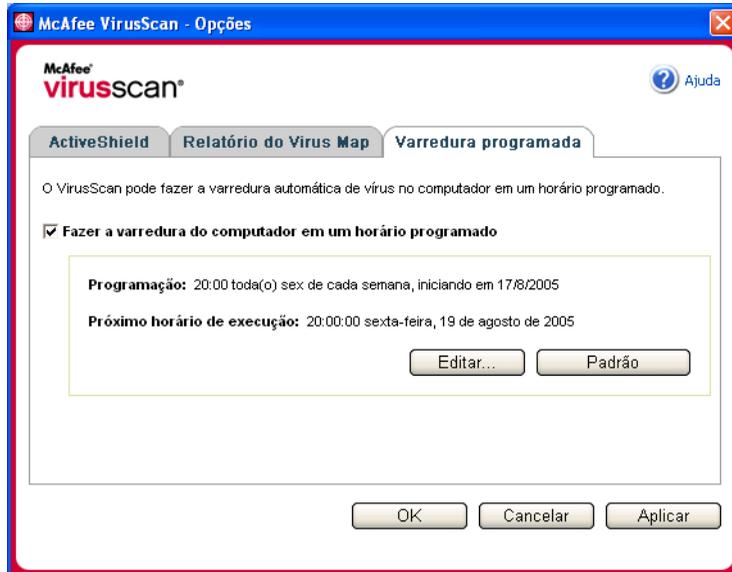



Figura 2-11. Opções de varredura programada

3 Marque a caixa de seleção **Fazer a varredura do computador em um horário programado** para ativar a varredura automática.

4 Especifique uma programação para a varredura automática:

- Para aceitar a programação padrão (toda sexta-feira, às 20h), clique em **OK**.
- Para editar a programação:

  a. Clique em **Editar**.

  b. Selecione a freqüência da varredura do computador na lista **Programar tarefa** e escolha opções adicionais na área dinâmica abaixo:

  Diariamente - especifique o número de dias entre as varreduras.

  Semanalmente (padrão) - especifique o número de semanas entre as varreduras, bem como os dias da semana.

  Mensalmente - especifique em qual dia do mês será feita a varredura. Clique em **Selecionar meses** para especificar os meses em que a varredura será feita e clique em **OK**.

  Uma vez - especifique em qual data a varredura será feita.

NOTA
Não há suporte para as seguintes opções do Agendador do Windows:
Ao inicializar o sistema, **Quando ocioso** e **Mostrar vários agendamentos**. O último agendamento permitido permanecerá ativado até você selecionar uma das opções válidas.

c. Na caixa **Hora de início**, selecione a hora do dia em que a varredura do computador será feita.

d. Para selecionar opções avançadas, clique em **Avançado**.

A caixa de diálogo **Opções de programação avançadas** será aberta.

i. Especifique uma data de início, data de término, duração, hora de término e se deseja interromper a tarefa em uma hora específica caso a varredura ainda esteja sendo executada.

ii. Clique em **OK** para salvar as alterações e fechar a caixa de diálogo. Caso contrário, clique em **Cancelar**.

5. Clique em **OK** para salvar as alterações e fechar a caixa de diálogo. Caso contrário, clique em **Cancelar**.
6. Para retornar à programação padrão, clique em **Padrão**. Caso contrário, clique em **OK**.

Entendendo as detecções de ameaças

Para a maioria dos vírus, cavalos de Tróia e worms, o mecanismo de varredura tenta limpar o arquivo automaticamente. Você pode especificar como gerenciará os arquivos infectados, inclusive se deseja enviá-los aos laboratórios AVERT da McAfee para serem pesquisados. Se o mecanismo de varredura detectar um programa potencialmente indesejado, tente limpá-lo manualmente, colocá-lo em quarentena ou excluí-lo (o envio para a AVERT não está disponível).

Para gerenciar vírus ou programas potencialmente indesejados:

1. Se um arquivo for exibido na **Lista de arquivos detectados**, clique na caixa de seleção ao lado do arquivo para selecioná-lo.

   NOTA
   Se aparecer mais de um arquivo na lista, você poderá marcar a caixa de seleção ao lado da lista **Nome do arquivo** para executar a mesma ação em todos os arquivos. Também é possível clicar no nome do arquivo na lista **Informações sobre a varredura** para exibir os detalhes da Biblioteca de informações sobre vírus.

2. Se o arquivo for um programa potencialmente indesejado, clique em **Limpar** para tentar limpá-lo.

3 Se a varredura não puder limpar o arquivo, clique em **Quarentena** para criptografar e isolar temporariamente arquivos infectados e suspeitos no diretório de quarentena até que uma ação adequada possa ser executada. (Consulte *Gerenciando arquivos em quarentena* na página 41 para obter detalhes.)

4 Se o mecanismo de varredura não conseguir limpar o arquivo ou colocá-lo em quarentena, execute uma destas ações:

- Clique em **Excluir** para remover o arquivo.
- Clique em **Cancelar** para fechar a caixa de diálogo sem realizar qualquer ação.

Se a varredura não conseguir limpar ou excluir o arquivo detectado, consulte a Biblioteca de informações sobre vírus em http://us.mcafee.com/virusInfo/default.asp para obter instruções sobre a exclusão manual do arquivo.

Se o arquivo detectado não permitir que você utilize a conexão com a Internet ou mesmo o computador, tente usar um Disco de resgate para iniciar o computador. Em muitos casos, o Disco de resgate pode iniciar o computador que foi desativado pelo arquivo detectado. Consulte *Criando um disco de resgate* na página 42 para obter detalhes.

Para obter mais ajuda, consulte o Atendimento ao cliente da McAfee em http://www.mcafeehelp.com/.

Gerenciando arquivos em quarentena

O recurso Quarentena criptografa e isola temporariamente os arquivos infectados e suspeitos no diretório de quarentena até que uma ação adequada possa ser executada. Após ser limpo, o arquivo em quarentena pode ser restaurado para o local original.

Para gerenciar um arquivo em quarentena:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Gerenciar arquivos em quarentena**.

   Uma lista de arquivos em quarentena é exibida (Figura 2-12).

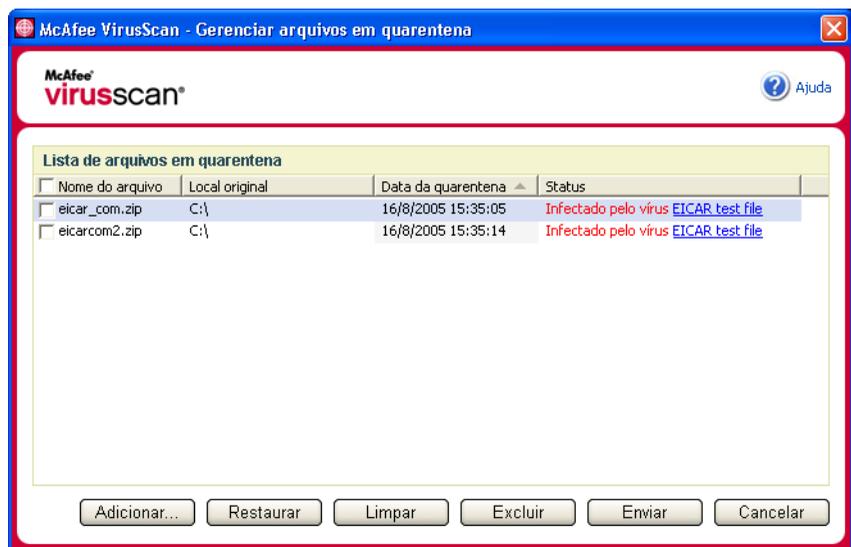



Figura 2-12. Caixa de diálogo Gerenciar arquivos em quarentena

2 Marque as caixas de seleção ao lado dos arquivos a serem limpos.

   NOTA
   Se aparecer mais de um arquivo na lista, você poderá marcar a caixa de seleção ao lado da lista **Nome do arquivo** para executar a mesma ação em todos os arquivos. Você também pode clicar no nome do vírus na lista **Status** para exibir os detalhes da Biblioteca de informações sobre vírus.

   Ou clique em **Adicionar**, selecione um arquivo suspeito para adicionar à lista de quarentena, clique em **Abrir** e selecione-o na lista de quarentena.

3 Clique em **Limpar**.

4 Se o arquivo estiver limpo, clique em **Restaurar** para movê-lo de volta ao local de origem.

5 Se o VirusScan não conseguir limpar o vírus, clique em **Excluir** para remover o arquivo.

6 Se o VirusScan não conseguir limpar ou excluir o arquivo e se o arquivo não for um programa potencialmente indesejado, você poderá enviá-lo à McAfee AntiVirus Emergency Response Team (AVERT™) para que seja pesquisado:

   a Atualize os arquivos de assinatura de vírus, caso tenham sido recebidos há mais de duas semanas.

   b Verifique a sua assinatura.

   c Selecione o arquivo e clique em **Enviar** para enviar o arquivo à AVERT.

   O VirusScan envia o arquivo em quarentena como um anexo de mensagem de e-mail contendo o seu endereço de e-mail, país, versão de software, sistema operacional, nome e local original do arquivo. O tamanho máximo para envio é um único arquivo de 1,5 MB por dia.

7 Clique em **Cancelar** para fechar a caixa de diálogo sem realizar nenhuma ação.

Criando um disco de resgate

O Disco de resgate é um utilitário que cria um disquete inicializável a ser utilizado para iniciar o computador e fazer a varredura de vírus quando um vírus impede a inicialização normal.

NOTA
É necessário estar conectado à Internet para fazer o download da imagem do Disco de resgate. Além disso, o Disco de resgate está disponível somente para computadores com partições de unidades de disco rígido FAT (FAT 16 e FAT 32). Ele é desnecessário para partições NTFS.

Para criar um Disco de resgate:

1 Em um computador não infectado, insira um disquete não infectado na unidade A. Convém usar a opção Fazer varredura para assegurar que não existem vírus no computador e no disquete. (Consulte *Fazendo a varredura manual de vírus e outras ameaças* na página 33 para obter detalhes.)

2 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Criar um Disco de resgate**.

A caixa de diálogo **Criar Disco de resgate** é exibida (Figura 2-13).

Figura 2-13. Caixa de diálogo Criar um Disco de resgate

3 Clique em **Criar** para criar o Disco de resgate.

Ao criar um Disco de resgate pela primeira vez, uma mensagem informa que é preciso fazer o download do arquivo de imagem do Disco de resgate. Clique em **OK** para fazer o download do componente agora ou clique em **Cancelar** para fazê-lo mais tarde.

Uma mensagem de aviso informa que o conteúdo do disquete será perdido.

4 Clique em **Sim** para continuar a criação do Disco de resgate.

O status da criação é exibido na caixa de diálogo **Criar um Disco de resgate**.

5 Quando a mensagem "Disco de resgate criado com êxito" for exibida, clique em **OK** e feche a caixa de diálogo **Criar Disco de resgate**.

6 Remova o Disco de resgate da unidade, proteja-o contra gravação e armazene-o em um local seguro.

Protegendo um Disco de resgate contra gravação

Para proteger um Disco de resgate contra gravação:

1 Coloque o disquete com o lado do rótulo para baixo (o círculo de metal deve estar visível).

2 Localize a lingüeta de proteção contra gravação. Deslize a lingüeta para que o orifício fique visível.

Usando um Disco de resgate

Para usar um Disco de resgate:

1. Desligue o computador infectado.
2. Insira o Disco de resgate na unidade.
3. Ligue o computador.

   Uma janela cinza com várias opções é exibida.
4. Escolha a opção que melhor atende às suas necessidades pressionando as teclas de função (por exemplo, F2, F3).

   NOTA
   Se você não pressionar nenhuma tecla, o Disco de resgate será inicializado automaticamente em 60 segundos.

Atualizando um Disco de resgate

O Disco de resgate deve ser atualizado regularmente. Para atualizar o Disco de resgate, siga as mesmas instruções de criação de um novo Disco de resgate.

Relatando vírus automaticamente

Agora é possível enviar, de forma anônima, informações de controle de vírus para serem incluídas no World Virus Map. Ative automaticamente esse recurso seguro e gratuito durante a instalação do VirusScan (na caixa de diálogo **Relatório do Virus Map**) ou a qualquer momento na guia **Relatório do Virus Map** da caixa de diálogo **Opções do VirusScan**.

Relatando ao World Virus Map

Para relatar automaticamente informações sobre vírus ao World Virus Map:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.

   A caixa de diálogo **Opções do VirusScan** será aberta.

2 Clique na guia **Relatório do Virus Map** (Figura 2-14).

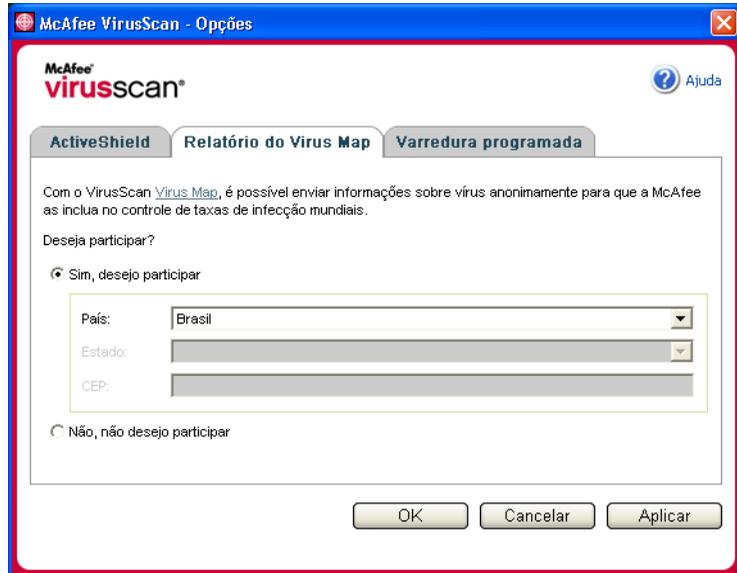



Figura 2-14. Opções de relatório do Virus Map

3 Aceite a opção padrão **Sim, desejo participar** para enviar anonimamente as informações de vírus à McAfee e incluí-las no World Virus Map de taxas de infecção mundiais. Caso contrário, selecione **Não, não desejo participar** para impedir o envio de informações.

4 Se estiver nos Estados Unidos, selecione o estado e informe o código de endereçamento postal correspondente ao local onde o seu computador se encontra. Caso contrário, o VirusScan tenta selecionar automaticamente o país em que o seu computador está localizado.

5 Clique em **OK**.

Exibindo o World Virus Map

Sendo participante ou não do World Virus Map, é possível exibir as taxas de infecções mundiais mais recentes usando o ícone da McAfee na bandeja de sistema do Windows.

Para exibir o World Virus Map:

- Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e, em seguida, clique em **World Virus Map**.

  A página da Web do **World Virus Map** é exibida (Figura 2-15).

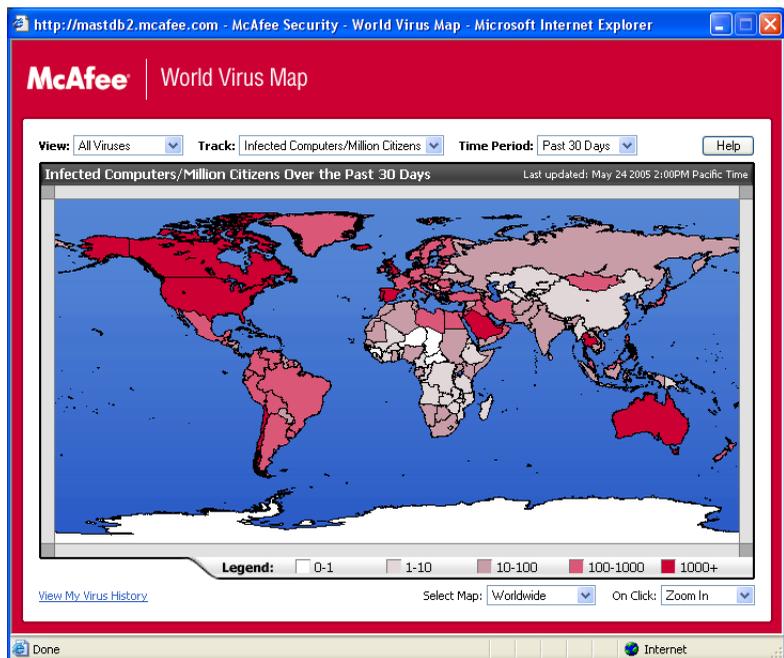



Figura 2-15. World Virus Map

Por padrão, o World Virus Map exibe o número de computadores infectados mundialmente nos últimos 30 dias e também a data em que os dados de relatórios foram atualizados pela última vez. É possível alterar o modo de visualização do mapa para exibir o número de arquivos infectados ou alterar o período, exibindo somente os resultados dos últimos 7 dias ou das últimas 24 horas.

A seção **Rastreamento de vírus** lista totais acumulados do número de arquivos examinados e infectados e de computadores infectados que foram relatados desde a data exibida.

Atualizando o VirusScan

Quando você está conectado à Internet, o VirusScan procura automaticamente atualizações a cada quatro horas. Semanalmente, faz o download automático das atualizações de definições de vírus, instalando-as sem interrupção do trabalho.

Os arquivos de definições de vírus possuem aproximadamente 100 KB e, portanto, causam impacto mínimo no desempenho do sistema durante o processo de download.

Se ocorrer uma atualização de produto ou epidemia de vírus, um alerta será exibido. Ao receber o alerta, faça a atualização do VirusScan para remover a ameaça de epidemia de vírus.

Verificando atualizações automaticamente

O McAfee SecurityCenter é automaticamente configurado para verificar atualizações de todos os serviços do McAfee a cada quatro horas quando você está conectado à Internet, notificando-o com alertas e sons. Por padrão, o SecurityCenter faz o download e instala automaticamente as atualizações disponíveis.

NOTA
Em alguns casos, é solicitado o reinício do computador para concluir a atualização. Verifique se salvou todo o seu trabalho e fechou todos os aplicativos antes de reiniciar o computador.

Verificando atualizações manualmente

Além de verificar as atualizações automaticamente a cada quatro horas quando se está conectado à Internet, também é possível verificar manualmente as atualizações a qualquer momento.

Para verificar as atualizações do VirusScan manualmente:

1. Verifique se o computador está conectado à Internet.
2. Clique com o botão direito do mouse no ícone da McAfee e, em seguida, clique em **Atualizações**.

   A caixa de diálogo **Atualizações do SecurityCenter** será aberta.
3. Clique em **Verificar agora**.

   Se houver uma atualização, a caixa de diálogo **Atualizações do VirusScan** será aberta (Figura 2-16 na página 48). Clique em **Atualizar** para continuar.

   Se nenhuma atualização estiver disponível, será aberta uma caixa de diálogo informando que o VirusScan está atualizado. Clique em **OK** para fechar a caixa de diálogo.

Figura 2-16. Caixa de diálogo Atualizações

4 Se solicitado, efetue logon no site da Web. O **Assistente de atualização** instala automaticamente a atualização.

5 Clique em **Concluir** quando a instalação da atualização estiver concluída.

NOTA
Em alguns casos, é solicitado o reinício do computador para concluir a atualização. Verifique se salvou todo o seu trabalho e fechou todos os aplicativos antes de reiniciar o computador.

McAfee Personal Firewall Plus 3

Bem-vindo ao McAfee Personal Firewall Plus.

O software McAfee Personal Firewall Plus oferece proteção avançada para seu computador e seus dados pessoais. O Personal Firewall estabelece uma barreira entre o seu computador e a Internet, monitorando de forma silenciosa o tráfego da Internet em busca de atividades suspeitas.

Ele oferece os seguintes recursos:

- Defesa contra possíveis sondagens e ataques de hackers
- Defesas antivírus adicionais
- Monitoramento da atividade da rede e da Internet
- Alerta sobre eventos potencialmente hostis
- Informações detalhadas sobre tráfego suspeito na Internet
- Integração da funcionalidade Hackerwatch.org, incluindo a geração de relatórios de eventos, ferramentas de autoteste e o recurso de envio de eventos relatados por e-mail para outras autoridades on-line
- Recursos detalhados de rastreamento e pesquisa de eventos

Novos recursos

- **Suporte avançado a jogos**
  O McAfee Personal Firewall Plus protege o computador contra tentativas de invasão e atividades suspeitas durante jogos de tela cheia, mas pode ocultar os alertas se detectar tentativas de invasão ou atividades suspeitas. Os alertas vermelhos são exibidos depois que você sai do jogo.

- **Manipulação aprimorada de acesso**
  O McAfee Personal Firewall Plus permite que os usuários concedam dinamicamente aos aplicativos acesso temporário à Internet. O acesso é restrito ao tempo decorrido entre a inicialização e o encerramento do aplicativo. Quando o Personal Firewall detecta um programa desconhecido tentando comunicação com a Internet, um alerta vermelho oferece a opção de conceder ao aplicativo o acesso temporário à Internet.

- **Controle de segurança aprimorado**
  A execução do recurso de Bloqueio do McAfee Personal Firewall Plus permite bloquear momentaneamente todo o tráfego de entrada e saída da Internet entre o computador e a Internet. Os usuários podem ativar e desativar o Bloqueio em três locais do Personal Firewall.

- **Opções aprimoradas de recuperação**
  As Opções de redefinição permitem restaurar automaticamente as configurações padrão do Personal Firewall. Se o Personal Firewall exibir um comportamento insatisfatório que não possa ser corrigido, é possível desfazer as configurações atuais e retornar às configurações padrão do produto.

- **Proteção à conectividade com a Internet**
  Para evitar que um usuário inadvertidamente desabilite sua própria conexão com a Internet, a opção de proibir um endereço da Internet é excluída em um alerta azul quando o Personal Firewall detecta uma conexão da Internet originada de um servidor DHCP ou DNS. Se o tráfego de entrada não for proveniente de um servidor DHCP ou DNS, a opção será exibida.

- **Integração aprimorada com o HackerWatch.org**
  A notificação de possíveis hackers agora ficou ainda mais fácil. O McAfee Personal Firewall Plus aprimora a funcionalidade do HackerWatch.org, que inclui o envio de eventos potencialmente mal-intencionados para o banco de dados.

- **Manipulação estendida inteligente de aplicativos**
  Quando um aplicativo busca acesso à Internet, o Personal Firewall primeiro verifica se reconhece o aplicativo como confiável ou mal-intencionado. Se o aplicativo for reconhecido como confiável, o Personal Firewall permitirá automaticamente o acesso à Internet para que você não precise fazê-lo.

- **Detecção avançada de cavalos de Tróia**
  O McAfee Personal Firewall Plus combina o gerenciamento de conexão de aplicativos com um banco de dados avançado para detectar e impedir que aplicativos potencialmente mal-intencionados, como cavalos de Tróia, acessem a Internet e transmitam seus dados pessoais.

- **Rastreamento visual aprimorado**
  O rastreamento visual inclui mapas gráficos de fácil leitura, que mostram a origem de tráfego e de ataques hostis em todo o mundo, inclusive informações detalhadas sobre contatos/proprietários de endereços IP de origem.

- **Mais fácil de usar**
  O McAfee Personal Firewall Plus inclui um Assistente de configuração e um Tutorial do usuário para ajudar o usuário a configurar e usar o firewall. Embora o produto tenha sido criado para ser usado sem intervenção, a McAfee oferece aos usuários vários recursos para que eles entendam e avaliem o que o firewall tem a oferecer.

- **Detecção aprimorada de invasões**
  O Sistema de detecção de invasão (IDS) do Personal Firewall detecta padrões de ataques comuns e outras atividades suspeitas. A detecção de invasões monitora todos os pacotes de dados em busca de transferências de dados ou métodos de transferência suspeitos e os inclui no registro de eventos.

- **Análise avançada de tráfego**
  O McAfee Personal Firewall Plus oferece aos usuários uma visão dos dados que entram e saem de seus computadores e exibe conexões de aplicativos, incluindo aqueles que estão ativamente "na escuta" em busca de conexões abertas. Isso permite que os usuários vejam e combatam os aplicativos que possam estar propensos a invasão.

Removendo outros firewalls

Antes de instalar o software do McAfee Personal Firewall Plus, é necessário remover todos os demais programas de firewall do computador. Siga as instruções de desinstalação do programa de firewall para executar esse procedimento.

> **NOTA**
> Se você usa o Windows XP, não é necessário desativar o recurso incorporado de firewall antes de instalar o McAfee Personal Firewall Plus. Mas, mesmo assim, recomendamos que você o desative. Do contrário, você não receberá eventos no registro de Eventos de entrada do McAfee Personal Firewall Plus.

Definindo o firewall padrão

O McAfee Personal Firewall é capaz de gerenciar as permissões e o tráfego dos aplicativos da Internet em seu computador, mesmo que o Windows Firewall esteja sendo executado.

Quando instalado, o McAfee Personal Firewall desativa automaticamente o Windows Firewall e se define como o firewall padrão. Assim, você receberá apenas a funcionalidade e as mensagens do McAfee Personal Firewall. Se, depois disso, você ativar o Windows Firewall no centro de segurança ou no painel de controle do Windows, permitindo que os dois firewalls sejam executados no computador, poderá haver perda parcial de dados no registro do Firewall, bem como mensagens duplicadas de status e de alerta.

NOTA

Se os dois firewalls estiverem ativados, o McAfee Personal Firewall não mostrará todos os endereços IP bloqueados na guia Eventos de entrada. O Windows Firewall intercepta e bloqueia a maioria desses eventos, evitando que o McAfee Personal Firewall os detecte e registre. Entretanto, o McAfee Personal Firewall pode bloquear o tráfego adicional com base em outros fatores de segurança e esse tráfego será registrado.

Por padrão, o registro é desativado no Windows Firewall. No entanto, para manter os dois firewalls ativados, é possível ativar o registro do Windows Firewall. O registro padrão do Windows Firewall é C:\Windows\pfirewall.log

Para assegurar que o computador estará protegido por ao menos um firewall, o Windows Firewall é reativado automaticamente quando o McAfee Personal Firewall é desinstalado.

Se você desativar o McAfee Personal Firewall ou definir o nível de segurança como **Aberto** sem ativar manualmente o Windows Firewall, toda a proteção do firewall será removida, com exceção dos aplicativos bloqueados anteriormente.

Definindo o nível de segurança

Você pode configurar opções de segurança para indicar como o Personal Firewall reagirá quando detectar um tráfego indesejado. Por padrão, o nível de segurança **Padrão** é ativado. No nível de segurança **Padrão**, quando um aplicativo solicita acesso à Internet e você o concede, está fornecendo acesso total ao aplicativo. O acesso total permite que o aplicativo envie e receba dados não solicitados em portas que não sejam do sistema.

Para definir as configurações de segurança:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Opções**.
2. Clique no ícone **Configurações de segurança**.
3. Defina o nível de segurança movendo o botão deslizante para o nível desejado.

   O nível de segurança varia de Bloqueado a Aberto:

   - **Bloqueado —** Todas as conexões da Internet no computador estão fechadas. Use esta configuração para bloquear as portas definidas como abertas na página Serviços do sistema.

- **Segurança rígida —** Quando um aplicativo solicita um tipo específico de acesso à Internet (por exemplo, Somente acesso de saída), é possível permitir ou proibir ao aplicativo a conexão à Internet. Se o aplicativo solicitar posteriormente Acesso total, você poderá conceder Acesso total ou limitá-lo a Somente acesso de saída.

- **Segurança padrão (recomendada) —** Quando um aplicativo solicita e recebe acesso à Internet, ele recebe acesso total à Internet para manipular o tráfego de entrada e de saída.

- **Segurança confiável —** Todos os aplicativos são considerados confiáveis quando tentam acessar a Internet pela primeira vez. No entanto, é possível configurar o Personal Firewall para usar alertas que notifiquem sobre novos aplicativos no computador. Use esta configuração caso desconfie que alguns jogos ou arquivos de mídia não estejam funcionando.

- **Aberto —** O firewall está desativado. Essa configuração permite que todo o tráfego passe pelo Personal Firewall sem ser filtrado.

  NOTA
  Os aplicativos bloqueados anteriormente continuarão bloqueados se o firewall estiver definido como **Aberto** ou **Bloqueado**. Para evitar que isso ocorra, altere as permissões do aplicativo para **Permitir acesso total** ou exclua a regra de permissão **Bloqueado** da lista **Aplicativos da Internet**.

4 Selecione configurações adicionais de segurança:

  NOTA
  Se o computador for executado no Windows XP e vários usuários do XP tiverem sido adicionados, essas opções estarão disponíveis somente se você tiver efetuado logon como administrador.

- **Gravar os eventos da detecção de invasão (IDS) no registro de Eventos de entrada —** Se esta opção for selecionada, os eventos detectados pelo IDS serão exibidos no registro de Eventos de entrada. O Sistema de detecção de invasão (IDS) detecta tipos comuns de ataques e outras atividades suspeitas. A detecção de invasão monitora todos os pacotes de dados de entrada e de saída em busca de métodos de transferência ou transferências de dados suspeitos. Ela compara esses dados com um banco de dados de "assinaturas" e rejeita automaticamente os pacotes vindos de computadores ofensivos.

  O IDS procura padrões de tráfego específicos usados pelos invasores. A detecção também verifica todos os pacotes recebidos pelo computador para detectar o tráfego de ataques suspeitos ou conhecidos. Por exemplo, quando encontra pacotes ICMP, o Personal Firewall os analisa em busca de padrões de tráfego suspeito, comparando o tráfego ICMP com padrões de ataques conhecidos.

- **Aceitar solicitações de ping ICMP** — O tráfego ICMP é usado principalmente para executar rastreamentos e pings. O recurso de ping normalmente é usado para executar um teste rápido antes de estabelecer comunicações. Se você estiver usando ou já tiver usado um programa de compartilhamento de arquivos ponto a ponto, talvez receba muitas solicitações de ping. Se esta opção for selecionada, o Personal Firewall permitirá todas as solicitações de ping sem incluí-las no registro de Eventos de entrada. Se esta opção ficar desmarcada, o Personal Firewall bloqueará todas as solicitações de ping e as incluirá no registro de Eventos de entrada.
- **Permitir que usuários restritos alterem as configurações do Personal firewall** — Se o computador estiver executando o Windows XP ou o Windows 2000 Professional com vários usuários, selecione essa opção para permitir que os usuários restritos do XP modifiquem as configurações do Personal Firewall.

5 Clique em **OK** ao terminar de fazer as alterações.

Testando o McAfee Personal Firewall Plus

É possível testar a instalação do Personal Firewall para verificar possíveis vulnerabilidades a atividades suspeitas e invasões.

Para testar a instalação do Personal Firewall usando o ícone da McAfee na bandeja do sistema:

- Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows e selecione **Testar o firewall**.

O Personal Firewall inicia o Internet Explorer e acessa http://www.hackerwatch.org/, um site da Web mantido pela McAfee. Siga as instruções na página Hackerwatch.org Probe para testar o Personal Firewall.

Sobre a página Resumo

O Resumo do Personal Firewall contém quatro páginas:

- Resumo principal
- Resumo do aplicativo
- Resumo de eventos
- Resumo do HackerWatch

As páginas de resumo contêm vários relatórios sobre eventos de entrada recentes, status de aplicativos e a atividade de invasão mundial relatada pelo HackerWatch.org. Também é possível encontrar links para tarefas comuns executadas no Personal Firewall.

Para abrir a página Resumo principal no Personal Firewall:

- Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Exibir resumo** (Figura 3-1).

Figura 3-1. Página Resumo principal

Clique nestas opções para navegar para outras páginas de resumo:

Item	Descrição
Alterar exibição	Clique em **Alterar exibição** para abrir uma lista das páginas de resumo. Na lista, selecione uma página do Resumo para ser exibida.
Seta para a direita	Clique no ícone de seta para a direita para exibir a próxima página Resumo.
Seta para a esquerda	Clique no ícone de seta para a esquerda a fim de exibir a página de resumo anterior.
Principal	Clique neste ícone para retornar à página **Resumo principal**.

A página Resumo principal fornece as seguintes informações:

Item	Descrição
Configuração de segurança	O status da configuração de segurança indica o nível de segurança para o qual o firewall está definido. Clique no link para alterar o nível de segurança.
Eventos bloqueados	O status dos eventos bloqueados exibe o número de eventos que foram bloqueados no dia. Clique no link para exibir os detalhes dos eventos na página Eventos de entrada.
Alterações na regra do aplicativo	O status da regra do aplicativo mostra o número de regras de aplicativo que foram alteradas recentemente. Clique no link para exibir a lista de aplicativos permitidos e bloqueados e para modificar permissões de aplicativos.
O que há de novo?	**O que há de novo?** mostra o último aplicativo que recebeu acesso total à Internet.
Último evento	**Último evento** esta opção mostra os eventos de entrada mais recentes. Clique em um link para rastrear um evento ou para confiar no endereço IP. A confiança em um endereço IP permite que todo o tráfego proveniente desse endereço acesse o seu computador.
Relatório diário	**Relatório diário** exibe o número de eventos de entrada que o Personal Firewall bloqueou no dia, na semana e no mês. Clique no link para exibir detalhes do evento na página Eventos de entrada.
Aplicativos ativos	**Aplicativos ativos** exibe os aplicativos que estão em execução no computador e acessando a Internet. Clique em um aplicativo para exibir os endereços IP que o aplicativo está acessando.
Tarefas comuns	Clique em um link em **Tarefas comuns** para passar às páginas do Personal Firewall nas quais é possível exibir a atividade do firewall e executar tarefas.

Para exibir a página Resumo do aplicativo:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Exibir resumo.**
2. Clique em **Alterar exibição** e selecione **Resumo do aplicativo**.

A página Resumo do aplicativo fornece as seguintes informações:

Item	Descrição
Monitor de tráfego	A opção **Monitor de tráfego** mostra as conexões de entrada e saída da Internet nos últimos quinze minutos. Clique no gráfico para exibir os detalhes da monitoração do tráfego.
Aplicativos ativos	**Aplicativos ativos** mostra o uso de largura de banda dos aplicativos mais ativos do computador nas últimas 24 horas. **Aplicativo** - o aplicativo que está acessando a Internet. **%** - a porcentagem de largura de banda usada pelo aplicativo. **Permissão** - o tipo de acesso à Internet permitido ao aplicativo. **Regra criada** - quando a regra do aplicativo foi criada.
O que há de novo?	**O que há de novo?** mostra o último aplicativo que recebeu acesso total à Internet.
Aplicativos ativos	**Aplicativos ativos** exibe os aplicativos que estão em execução no computador e acessando a Internet. Clique em um aplicativo para exibir os endereços IP que o aplicativo está acessando.
Tarefas comuns	Clique em um link em **Tarefas comuns** para passar às páginas do Personal Firewall nas quais é possível exibir o status do aplicativo e executar as tarefas relacionadas ao aplicativo.

Para exibir a página Resumo de eventos:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Exibir resumo.**
2. Clique em **Alterar exibição** e selecione **Resumo de eventos**.

A página Resumo de eventos oferece as seguintes informações:

Item	Descrição
Comparação de portas	**Comparação de portas** mostra um gráfico de pizza das portas mais solicitadas do computador nos últimos 30 dias. Clique em um nome de porta para exibir os detalhes da página Eventos de entrada. Também é possível mover o ponteiro do mouse sobre o número da porta para exibir a descrição.
Principais infratores	**Principais infratores** mostra os endereços IP bloqueados com mais freqüência, quando o último evento de entrada ocorreu em cada endereço e o número total de eventos de entrada de cada endereço nos últimos trinta dias. Clique em um evento para exibir os detalhes na página Eventos de entrada.

Item	Descrição
Relatório diário	**Relatório diário** exibe o número de eventos de entrada que o Personal Firewall bloqueou no dia, na semana e no mês. Clique em um número para exibir os detalhes do evento no registro de Eventos de entrada.
Último evento	**Último evento** esta opção mostra os eventos de entrada mais recentes. Clique em um link para rastrear um evento ou para confiar no endereço IP. A confiança em um endereço IP permite que todo o tráfego proveniente desse endereço acesse o seu computador.
Tarefas comuns	Clique em um link em **Tarefas comuns** para passar às páginas do Personal Firewall nas quais é possível exibir os detalhes dos eventos e executar as tarefas a eles relacionadas.

Para exibir a página Resumo do HackerWatch:

1 Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Exibir resumo.**

2 Clique em **Alterar exibição** e selecione **Resumo do HackerWatch.**

A página Resumo do HackerWatch fornece as seguintes informações:

Item	Descrição
Atividade mundial	**Atividade mundial** mostra um mapa-múndi que identifica as atividades bloqueadas recentemente monitoradas pelo HackerWatch.org. Clique no mapa para abrir o mapa de análise de ameaças globais no HackerWatch.org.
Rastreamento de eventos	**Rastreamento de eventos** mostra o número de eventos de entrada enviados para o HackerWatch.org.
Atividade global de porta	**Atividade global de porta** mostra as principais portas que, nos últimos 5 dias, demonstraram ser ameaças. Clique em uma porta para exibir seu número e sua descrição.
Tarefas comuns	Clique em um link em **Tarefas comuns** para passar às páginas do HackerWatch.org nas quais é possível obter mais informações sobre a atividade de hackers no mundo todo.

Sobre a página Aplicativos da Internet

Use a página Aplicativos da Internet para exibir a lista de aplicativos permitidos e bloqueados.

Para iniciar a página Aplicativos da Internet:

- Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Aplicativos** (Figura 3-2).

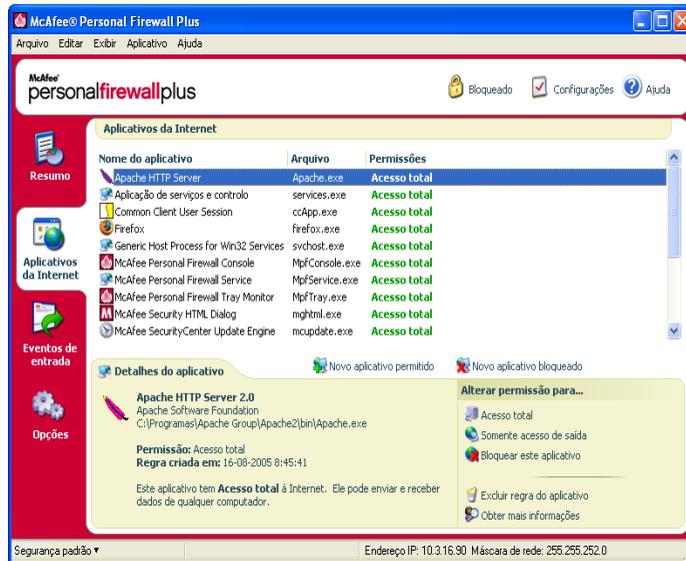



Figura 3-2. Página Aplicativos da Internet

A página Aplicativos da Internet oferece as seguintes informações:

- Nomes dos aplicativos
- Nomes dos arquivos
- Níveis de permissão atuais
- Detalhes do aplicativo: nome e versão do aplicativo, nome da empresa, nome do caminho, permissão, marcas de data e hora e explicações dos tipos de permissão.

Alterando regras de aplicativos

O Personal Firewall permite alterar o acesso às regras dos aplicativos.

Para alterar uma regra do aplicativo:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **Personal Firewall** e selecione **Aplicativos da Internet**.
2. Na lista **Aplicativos da Internet**, clique com o botão direito do mouse na regra de um aplicativo e selecione um nível diferente:
   - **Permitir acesso total —** permite que o aplicativo estabeleça conexões de entrada e saída da Internet.
   - **Somente acesso de saída —** permite que o aplicativo estabeleça apenas uma conexão de saída da Internet.
   - **Bloquear este aplicativo —** não permite ao aplicativo o acesso à Internet.

     NOTA
     Os aplicativos bloqueados anteriormente continuam bloqueados quando o firewall está configurado como **Aberto** ou **Bloqueado**. Para evitar que isso aconteça, altere a regra de acesso do aplicativo para **Acesso total** ou exclua a regra de permissão **Bloqueado** da lista **Aplicativos da Internet**.

Para excluir uma regra do aplicativo:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e selecione **Aplicativos da Internet**.
2. Na lista **Aplicativos da Internet**, clique com o botão direito do mouse na regra do aplicativo e selecione **Excluir regra do aplicativo**.

Na próxima vez que o aplicativo solicitar acesso à Internet, defina o nível de permissão para adicioná-lo à lista novamente.

Permitindo e bloqueando aplicativos da Internet

Para alterar a lista de aplicativos da Internet permitidos e bloqueados:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e selecione **Aplicativos da Internet**.
2. Na página Aplicativos da Internet, clique em uma das seguintes opções:
   - **Novo aplicativo permitido** — permite ao aplicativo o acesso total à Internet.
   - **Novo aplicativo bloqueado** — não permite o acesso de um aplicativo à Internet.
   - **Excluir regra do aplicativo** — remove uma regra do aplicativo.

Sobre a página Eventos de entrada

Use a página Eventos de entrada para exibir o registro de Eventos de entrada gerado quando o Personal Firewall bloqueia conexões de Internet não solicitadas.

Para iniciar a página Eventos de entrada:

- Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Eventos de entrada** (Figura 3-3).

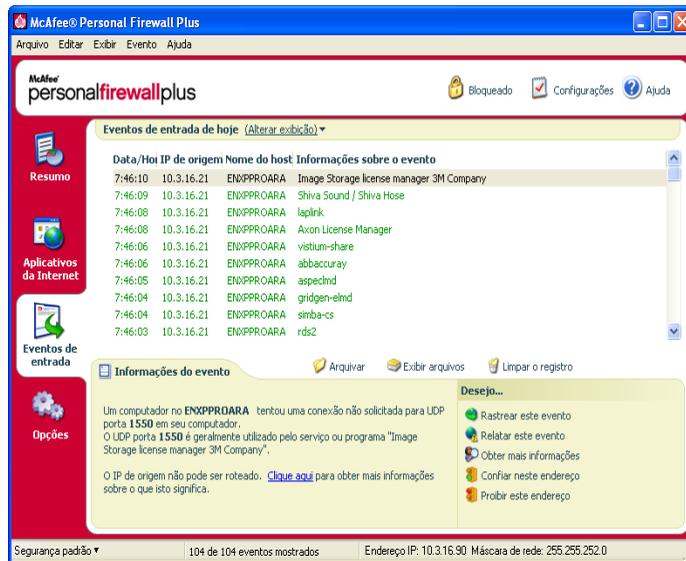



Figura 3-3. Página Eventos de entrada

A página Eventos de entrada oferece as seguintes informações:

- Marcas de data e hora
- IPs de origem
- Nomes de host
- Nomes de serviços ou de aplicativos
- Detalhes do evento: tipos de conexão, portas de conexão, IP ou nome do host e explicações de eventos de porta

Noções básicas sobre eventos

Sobre endereços IP

Os endereços IP são números: quatro números, cada um entre 0 e 255. Esses números identificam um local específico para onde o tráfego pode ser direcionado na Internet.

Tipos de endereço IP

Diversos endereços IP são incomuns por vários motivos:

Endereços IP não roteáveis — também chamados de "Espaço IP privado". Esses endereços IP não podem ser usados na Internet. Os blocos de endereços IP privados são 10.x.x.x, 172.16.x.x - 172.31.x.x e 192.168.x.x.

Endereços IP de loopback — os endereços de loopback são usados para fins de teste. O tráfego enviado a esse bloco de endereços IP volta para o dispositivo que gerou o pacote. Ele nunca sai do dispositivo e é usado principalmente para teste de hardware e software. O bloco de endereços IP de loopback é 127.x.x.x.

Endereço IP nulo — é um endereço inválido. Quando detectado, o Personal Firewall indica que o tráfego utilizou um endereço IP em branco. Geralmente isso indica que o remetente está deliberadamente ocultando a origem do tráfego. O remetente não poderá receber nenhuma resposta para esse tráfego, a não ser que o pacote seja recebido por um aplicativo que reconheça o conteúdo do pacote que conterá instruções específicas desse aplicativo. Qualquer endereço que inicie com 0 (0.x.x.x) é um endereço nulo. Por exemplo, 0.0.0.0 é um endereço IP nulo.

Eventos de 0.0.0.0

Quando são exibidos eventos do endereço IP 0.0.0.0, existem duas causas prováveis. A primeira, e mais comum, é que o computador recebeu um pacote inválido. A Internet nem sempre é 100% confiável e é comum haver pacotes com problemas. Como o Personal Firewall vê os pacotes antes que o TCP/IP possa validá-los, ele pode relatar esses pacotes como um evento.

A outra situação ocorre quando o IP de origem é fraudado ou falso. Os pacotes fraudados podem ser um sinal de que alguém está em busca de cavalos de Tróia no seu computador. O Personal Firewall bloqueia este tipo de atividade, portanto o computador está seguro.

Eventos de 127.0.0.1

Às vezes os eventos indicam o IP de origem como 127.0.0.1. Esse IP se chama endereço de loopback ou localhost.

Muitos programas legítimos usam o endereço de loopback para comunicação entre componentes. Por exemplo, é possível configurar muitos servidores de e-mail pessoal ou servidores Web por meio de uma interface da Web. Para acessar a interface, digite “http://localhost/” no navegador da Web.

O Personal Firewall permite o tráfego desses programas. Portanto, se você receber eventos de 127.0.0.1, é provável que o endereço IP de origem esteja fraudado ou seja falso. Os pacotes fraudados geralmente indicam que outro computador está em busca de cavalos de Tróia no seu computador. O Personal Firewall bloqueia essas tentativas de invasão; portanto, o computador está seguro.

Alguns programas, particularmente o Netscape 6.2 e posterior, exigem que o endereço 127.0.0.1 seja adicionado à lista de endereços IP confiáveis. Os componentes desses programas se comunicam entre si de uma maneira que o Personal Firewall não consegue determinar se o tráfego é local ou não.

No exemplo do Netscape 6.2, se você não confiar no 127.0.0.1, não poderá usar sua lista de amigos. Portanto, se você receber tráfego de 127.0.0.1 e todos os aplicativos do computador funcionarem normalmente, é sinal de que esse tráfego pode ser bloqueado sem problemas. Porém, se ocorrerem problemas com algum programa (como o Netscape), adicione o 127.0.0.1 à lista de endereços IP confiáveis do Personal Firewall.

Se isso resolver o problema, será necessário tomar uma decisão: se confiar no 127.0.0.1, o programa funcionará, mas você estará mais vulnerável a ataques fraudados. Se não confiar no endereço, o programa não funcionará, mas você continuará protegido contra determinado tráfego mal-intencionado.

Eventos de computadores na LAN

Os eventos podem ser gerados por computadores da rede local (LAN). Para indicar que esses eventos são gerados pela sua rede, o Personal Firewall os exibe em verde.

Na maioria das configurações de LAN corporativas, selecione **Tornar todos os computadores da sua LAN confiáveis** nas opções de endereços IP confiáveis.

Em algumas situações, a rede "local" pode ser tão perigosa quanto a Internet, especialmente se o computador for executado em uma rede DSL de banda larga ou modem a cabo. Nesse caso, não selecione **Tornar todos os computadores da sua LAN confiáveis**. Em vez disso, adicione os endereços IP dos computadores locais à lista de endereços IP confiáveis.

Eventos de endereços IP privados

Os endereços IP de formato 192.168.xxx.xxx, 10.xxx.xxx.xxx e 172.16.0.0 - 172.31.255.255 são chamados de não-roteáveis ou privados. Esses endereços IP nunca devem sair da sua rede e, na maioria das vezes, são confiáveis.

O bloco 192.168 xxx.xxx é usado com o Microsoft Internet Connection Sharing (ICS). Se estiver usando ICS e receber eventos desse bloco de endereços IP, poderá adicionar o endereço IP 192.168.255.255 à lista de endereços IP confiáveis. Isso tornará todo o bloco 192.168.xxx.xxx confiável.

Se você não estiver em uma rede privada e receber eventos desses intervalos de endereços IP, talvez o endereço IP de origem esteja fraudado ou seja falso. Os pacotes fraudados geralmente são um sinal de que alguém está fazendo uma varredura em busca de cavalos de Tróia. É importante lembrar que o Personal Firewall bloqueou essa tentativa e, portanto, seu computador está seguro.

Como os endereços IP privados se referem a computadores diferentes dependendo da rede em que você está, o relato desses eventos não traz nenhum benefício e, por isso, não é necessário fazê-lo.

Mostrando eventos no registro de Eventos de entrada

O registro de Eventos de entrada exibe os eventos de várias formas. A exibição padrão se limita aos eventos que ocorreram no dia atual. Você também pode exibir eventos que ocorreram na semana passada ou exibir o registro completo.

O Personal Firewall também permite exibir eventos de entrada de dias específicos, de endereços da Internet específicos (endereços IP) ou eventos que contenham as mesmas informações.

Para obter informações sobre um evento, clique nele para exibir as informações no painel **Informações sobre o evento**.

Mostrando os eventos de hoje

Use esta opção para analisar os eventos do dia.

Para mostrar os eventos de hoje:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Eventos de entrada**.
2. No registro de Eventos de entrada, clique com o botão direito do mouse em uma entrada, e, em seguida, clique em **Mostrar eventos de hoje**.

Mostrando os eventos desta semana

Use esta opção para analisar os eventos da semana.

Para mostrar os eventos da semana:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Eventos de entrada**.
2. No registro de Eventos de entrada, clique com o botão direito do mouse em uma entrada e, em seguida, clique em **Mostrar eventos desta semana**.

Mostrando o registro de Eventos de entrada completo

Use esta opção para analisar todos os eventos.

Para mostrar todos os eventos do registro de Eventos de entrada:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **Personal Firewall** e selecione **Eventos de entrada**.
2. No registro de Eventos de entrada, clique com o botão direito do mouse em uma entrada e, em seguida, clique em **Mostrar registro completo**.

   O registro de Eventos de entrada exibe todos os eventos do registro de Eventos de entrada.

Mostrando eventos de um dia específico.

Use esta opção para analisar os eventos de um dia específico.

Para mostrar os eventos de um dia:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Eventos de entrada**.
2. No registro de Eventos de entrada, clique com o botão direito do mouse em uma entrada e escolha **Mostrar somente eventos do dia selecionado**.

Mostrando eventos de um endereço da Internet específico.

Use esta opção para examinar outros eventos que se originam de um endereço da Internet específico.

Para mostrar eventos de um endereço da Internet:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e clique em **Eventos de entrada**.
2. No registro de Eventos de entrada, clique com o botão direito do mouse em uma entrada e, em seguida, clique em **Mostrar somente eventos do endereço da Internet selecionado**.

Mostrando eventos que compartilham informações idênticas.

Use esta opção para examinar outros eventos no registro de Eventos de entrada que tenham as mesmas informações do evento selecionado na coluna Informações sobre o evento. Você pode descobrir quantas vezes esse evento ocorreu e se ele é da mesma origem. A coluna Informações sobre o evento oferece uma descrição do evento e, se for conhecido, o programa ou o serviço comum que usam essa porta.

Para mostrar eventos que compartilham informações idênticas:

1 Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e clique em **Eventos de entrada**.

2 No registro de Eventos de entrada, clique com o botão direito do mouse em uma entrada e, em seguida, clique em **Mostrar somente eventos com as mesmas informações de evento**.

Respondendo a eventos de entrada

Além de analisar os detalhes sobre os eventos do registro de Eventos de entrada, é possível executar um rastreamento visual dos endereços IP de um evento desse registro ou obter detalhes do evento no site HackerWatch.org da comunidade on-line anti-hackers.

Rastreando o evento selecionado

Você pode tentar executar um rastreamento visual dos endereços IP de um evento contido no registro de Eventos de entrada.

Para rastrear um evento selecionado:

1 Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e selecione **Eventos de entrada**.

2 No registro de Eventos de entrada, clique no evento a ser rastreado e, em seguida, clique em **Rastrear o evento selecionado**. Também é possível clicar duas vezes no evento para rastreá-lo.

Por padrão, o Personal Firewall inicia o rastreamento visual usando o programa Visual Trace integrado ao Personal Firewall.

Obtendo informações do HackerWatch.org

Para obter informações do HackerWatch.org:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **Personal Firewall** e selecione **Eventos de entrada**.

2 Selecione a entrada do evento na página Eventos de entrada e clique em **Obter mais informações** no painel **Desejo**.

O seu navegador padrão da Web é iniciado e abre o site HackerWatch.org para recuperar informações sobre o tipo de evento e saber se ele deve ser relatado.

Relatando um evento

Para relatar um evento que parece ser um ataque ao seu computador:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e selecione **Eventos de entrada**.
2. Clique no evento que deseja relatar e, em seguida, clique em **Relatar este evento** no painel **Desejo**.

O Personal Firewall relata o evento para o site HackerWatch.org usando a sua ID exclusiva.

Inscrevendo-se no HackerWatch.org

Quando você abre a página Resumo pela primeira vez, o Personal Firewall contata o site HackerWatch.org para gerar a sua ID de usuário exclusiva. Se você for um usuário existente, a inscrição será validada automaticamente. Se você for um novo usuário, deverá inserir um apelido e seu endereço de e-mail e, em seguida, clicar no link de validação no e-mail de confirmação do site HackerWatch.org para poder usar os recursos de filtragem/envio de eventos por e-mail desse site.

É possível relatar eventos para o site HackerWatch.org sem validar a ID de usuário. No entanto, para filtrar eventos e enviá-los por e-mail para um amigo, é necessário inscrever-se nesse serviço.

A inscrição no serviço permite que os envios sejam rastreados e que você seja notificado se o HackerWatch.org precisar de mais informações ou de sua intervenção. A inscrição também é necessária porque precisamos confirmar todas as informações recebidas para que elas sejam úteis.

Todos os endereços de e-mail fornecidos ao site HackerWatch.org são mantidos como confidenciais. Se um ISP solicitar informações adicionais, essa solicitação será roteada pelo site HackerWatch.org. Seu endereço de e-mail nunca será revelado.

Confiando em um endereço

É possível usar a página Eventos de entrada para adicionar um endereço IP à lista de endereços IP confiáveis, permitindo, assim, a conexão permanente.

Se, na página de eventos de entrada, houver um evento contendo um endereço IP em que você precise confiar, determine que o Personal Firewall sempre permita conexões desse endereço.

Para adicionar um endereço IP à lista de endereços IP confiáveis:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e selecione **Eventos de entrada**.
2. Clique com o botão direito do mouse no evento cujo endereço IP deve ser confiável e clique em **Confiar no endereço IP de origem**.

Verifique se o endereço IP exibido na caixa de diálogo Confiar neste endereço está correto e clique em **OK**. O endereço IP será adicionado à lista de endereços IP confiáveis.

Para verificar se o endereço IP foi adicionado:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e selecione **Opções**.
2. Clique no ícone **IPs confiáveis e proibidos** e, em seguida, na guia **Endereços IP confiáveis**.

O endereço IP aparecerá marcado na lista de endereços IP confiáveis.

Proibindo um endereço

Um endereço IP que aparece no registro de Eventos de entrada indica que o tráfego desse endereço foi bloqueado. Portanto, proibir um endereço não garante proteção adicional, a menos que as portas do computador sejam abertas deliberadamente pelo recurso Serviços do sistema ou que o computador possua um aplicativo com permissão para receber tráfego.

Adicione um endereço IP à lista de endereços proibidos somente se houver uma ou mais portas que sejam deliberadamente abertas e se houver motivos para acreditar que o bloqueio seja necessário.

Se houver algum evento na página Eventos de entrada que contenha um endereço IP a ser proibido, é possível configurar o Personal Firewall para impedir sempre as conexões desse endereço.

É possível usar a página Eventos de entrada, que lista os endereços IP de todo o tráfego da Internet, para proibir um endereço IP suspeito de ser a origem de atividade suspeita ou não desejada na Internet.

Para adicionar um endereço IP à lista de endereços IP proibidos:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Eventos de entrada**.
2. A página Eventos de entrada lista os endereços IP de todo o tráfego de entrada da Internet. Selecione um endereço IP e execute um dos seguintes procedimentos:
   - Clique com o botão direito do mouse no endereço IP e selecione **Proibir o endereço IP de origem**.
   - No menu **Desejo**, clique em **Proibir este endereço**.

3 Na caixa de diálogo Adicionar regra de endereço IP proibido, use uma ou mais das configurações a seguir para determinar a regra de endereço IP proibido.

- **Endereço IP único**: O endereço IP a ser proibido. A entrada padrão é o endereço IP selecionado na página Eventos de entrada.
- **Intervalo de endereços IP**: Os endereços IP entre o endereço especificado em De endereço IP e o endereço IP especificado em Até endereço IP.
- **Fazer com que esta regra expire em**: Data e hora de expiração da regra do endereço IP proibido. Selecione os menus suspensos apropriados para selecionar a data e a hora.
- **Descrição**: Opcionalmente, descreva a nova regra.
- Clique em **OK**.

4 Na caixa de diálogo, clique em **Sim** para confirmar a configuração. Clique em **Não** para voltar à caixa de diálogo Adicionar regra de endereço IP proibido.

Quando detecta um evento proveniente de uma conexão proibida da Internet, o Personal Firewall emite um alerta de acordo com o método especificado na página Configurações de alerta.

Para verificar se o endereço IP foi adicionado:

1 Clique na guia **Opções**.

2 Clique no ícone **IPs confiáveis e proibidos** e, em seguida, clique na guia **Endereços IP proibidos**.

O endereço IP aparece marcado na lista de endereços IP proibidos.

Gerenciando o registro de Eventos de entrada

A página Eventos de entrada permite gerenciar os eventos do registro de Eventos de entrada gerados quando o Personal Firewall bloqueia o tráfego de Internet não solicitado.

Arquivando o registro de Eventos de entrada

É possível arquivar o registro de Eventos de entrada atual para salvar todos os eventos de entrada registrados, incluindo datas e horas, IPs de origem, nomes de host, portas e informações sobre eventos. O registro de Eventos de entrada deve ser arquivado periodicamente para impedir que fique muito grande.

Para arquivar o registro de Eventos de entrada:

1 Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Eventos de entrada**.

2 Na página Eventos de entrada, clique em **Arquivar**.

3. Na caixa de diálogo Arquivar registro, clique em **Sim** para continuar com a operação.

4. Clique em **Salvar** para salvar o arquivo no local padrão ou navegue até o local onde deseja salvá-lo.

Nota: Por padrão, o Personal Firewall arquiva automaticamente o registro de Eventos de entrada. Marque ou desmarque **Arquivar automaticamente os eventos registrados** na página Registro de eventos para ativar ou desativar a opção.

Exibindo um registro de eventos de entrada arquivado.

Você pode exibir qualquer registro de Eventos de entrada que tenha sido arquivado anteriormente. O arquivo salvo inclui datas e horários, IPs de origem, nomes de host, portas e informações sobre eventos relacionados aos eventos.

Para exibir um registro de Eventos de entrada arquivado:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Eventos de entrada**.

2. Na página Eventos de entrada, clique em **Exibir arquivos**.

3. Selecione ou procure o nome de arquivo e clique em **Abrir**.

Limpando o registro de Eventos de entrada

É possível limpar todas as informações do registro de Eventos de entrada.

AVISO: Se você limpar o registro de Eventos de entrada, ele não poderá ser recuperado. Se você acha que precisará do registro de eventos no futuro, arquive-o.

Para limpar o registro de Eventos de entrada:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **Personal Firewall** e selecione **Eventos de entrada**.

2. Na página Eventos de entrada, clique em **Limpar o registro**.

3. Clique em **Sim** na caixa de diálogo para limpar o registro.

Copiando um evento para a área de transferência

É possível copiar um evento para a área de transferência para poder colá-lo em um arquivo de texto usando o Bloco de notas.

Para copiar eventos para a área de transferência:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **Personal Firewall** e selecione **Eventos de entrada**.

2 Clique com o botão direito do mouse no evento do registro de Eventos de entrada.

3 Clique em **Copiar evento selecionado para a área de transferência**.

4 Iniciar o Bloco de notas.

   - Digite `notepad` na linha de comando ou clique no botão **Iniciar** do Windows, aponte para **Programas** e, em seguida, para **Acessórios**. Selecione **Bloco de notas**.

5 Clique em **Editar** e, em seguida, em Colar. O texto do evento será exibido no Bloco de notas. Repita essa etapa para todos os eventos necessários.

6 Salve o arquivo do Bloco de notas em um local seguro.

Excluindo o evento selecionado

É possível excluir eventos do registro de Eventos de entrada.

Para excluir eventos do registro de Eventos de entrada:

1 Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Eventos de entrada**.

2 Clique na entrada do evento a ser excluído na página Eventos de entrada.

3 No menu Editar, clique em **Excluir evento selecionado**. O evento é excluído do registro de Eventos de entrada.

Sobre alertas

Recomendamos que você se familiarize com os tipos de alertas que encontrará ao usar o Personal Firewall. Observe a seguir os tipos de alertas que podem ser exibidos e as possíveis respostas a serem escolhidas para reagir com segurança a um alerta.

NOTA
As recomendações sobre alertas ajudam a decidir como lidar com cada alerta. Para exibir recomendações nos alertas, clique na guia **Opções**, clique no ícone **Configurações de alerta** e selecione **Utilizar recomendações inteligentes** (o padrão) ou **Exibir somente as recomendações inteligentes** na lista **Recomendações inteligentes**.

Alertas vermelhos

Os alertas vermelhos contêm informações importantes que exigem atenção imediata.

- **Aplicativo de Internet bloqueado —** esse alerta será exibido se o Personal Firewall impedir o acesso de um aplicativo à Internet. Por exemplo, se for exibido um alerta de programa cavalo de Tróia, a McAfee impedirá automaticamente que esse programa acesse a Internet e recomendará que se faça uma varredura de vírus no computador.
- **O aplicativo deseja acessar a Internet —** esse alerta é exibido quando o Personal Firewall detecta tráfego da Internet ou da rede para novos aplicativos.
- **O aplicativo foi modificado —** esse alerta é exibido quando o Personal Firewall detecta a alteração de um aplicativo ao qual havia sido concedido o acesso à Internet. Se você não tiver atualizado o aplicativo recentemente, tome cuidado ao permitir que o aplicativo modificado acesse a Internet.
- **O aplicativo solicita acesso como servidor —** esse alerta é exibido quando o Personal Firewall detecta que um aplicativo ao qual você concedeu acesso à Internet anteriormente solicitou acesso à Internet como servidor.

NOTA

A configuração padrão das Atualizações automáticas do Windows XP SP2 faz o download e instala as atualizações do sistema operacional Windows e de outros programas da Microsoft em execução no computador sem avisar o usuário. Quando um aplicativo é modificado em uma atualização silenciosa do Windows, um alerta do McAfee Personal Firewall é exibido na primeira vez em que o aplicativo Microsoft é usado após a atualização.

IMPORTANTE

Você deve conceder acesso aos aplicativos que precisam acessar a Internet para executar atualizações de produtos on-line (como os serviços da McAfee) a fim de mantê-los atualizados.

Alerta Aplicativo da Internet bloqueado

Quando é exibido um alerta de cavalo de Tróia (Figura 3-4), o Personal Firewall nega automaticamente o acesso à Internet a esse programa e recomenda que seja feita a varredura no computador em busca de vírus. Se o McAfee VirusScan não estiver instalado, inicie o McAfee SecurityCenter.

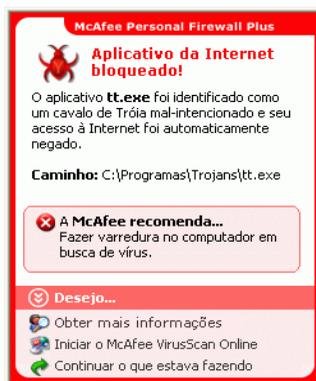



Figura 3-4. Alerta Aplicativo da Internet bloqueado

Veja uma breve descrição do evento e escolha uma das opções a seguir:

- Clique em **Obter mais informações** para obter detalhes sobre o evento por meio do registro de Eventos de entrada (consulte *Sobre a página Eventos de entrada* na página 61 para obter detalhes).
- Clique em **Iniciar o McAfee VirusScan** para fazer uma varredura de vírus no computador.
- Clique em **Continuar o que eu estava fazendo** se não desejar executar nenhuma ação além do que o Personal Firewall já tenha feito.
- Clique em **Conceder acesso de saída** para permitir uma conexão de saída (segurança **Rígida**).

Alerta O aplicativo deseja acessar a Internet

Se você tiver selecionado a segurança **Padrão** ou **Rígida** nas opções de Configurações de segurança, o Personal Firewall exibirá um alerta (Figura 3-5) quando detectar conexões da Internet ou da rede para aplicativos novos ou modificados.

Figura 3-5. Alerta O aplicativo deseja acessar a Internet

Se for exibido um alerta recomendando cuidado ao permitir que o aplicativo acesse a Internet, clique em **Clique aqui para obter mais informações** para obter mais informações sobre o aplicativo. Essa opção será exibida no alerta somente se o Personal Firewall estiver configurado para usar recomendações inteligentes.

A McAfee talvez não reconheça o aplicativo que está tentando obter acesso à Internet (Figura 3-6).

Figura 3-6. Alerta Aplicativo não reconhecido

Portanto, a McAfee não pode fornecer nenhuma recomendação sobre como lidar com o aplicativo. Para relatar o aplicativo à McAfee, clique em **Informe a McAfee sobre este programa**. Uma página da Web é exibida solicitando informações relacionadas ao aplicativo. Forneça o máximo de informações que souber.

As informações enviadas são usadas em conjunto com outras ferramentas de pesquisa pelos operadores do HackerWatch para determinar se um aplicativo merece estar relacionado em nosso banco de dados de aplicativos conhecidos e, em caso afirmativo, como ele deve ser tratado pelo Personal Firewall.

Veja uma breve descrição do evento e escolha uma das opções a seguir:

- Clique em **Conceder acesso** para permitir ao aplicativo uma conexão de entrada e saída da Internet.
- Clique em **Conceder acesso uma vez** para conceder ao aplicativo uma conexão temporária à Internet. O acesso é limitado ao tempo decorrido entre a inicialização e o encerramento do aplicativo.
- Clique em **Bloquear todo o acesso** para proibir uma conexão à Internet.
- Clique em **Conceder acesso de saída** para permitir uma conexão de saída (segurança **Rígida**).
- Clique em **Ajude-me a escolher** para exibir a Ajuda on-line sobre as permissões de acesso do aplicativo.

Alerta O aplicativo foi modificado

Se você tiver selecionado a segurança **Confiável**, **Padrão** ou **Rígida** nas opções de Configurações de segurança, o Personal Firewall exibirá um alerta (Figura 3-7) quando o Personal Firewall detectar a alteração de um aplicativo ao qual havia sido permitido o acesso à Internet. Se você não tiver atualizado este aplicativo recentemente, tome cuidado ao permitir o acesso deste aplicativo à Internet.

Figura 3-7. Alerta O aplicativo foi modificado

Veja uma breve descrição do evento e escolha uma das opções a seguir:

- Clique em **Conceder acesso** para permitir ao aplicativo uma conexão de entrada e saída da Internet.
- Clique em **Conceder acesso uma vez** para conceder ao aplicativo uma conexão temporária à Internet. O acesso é limitado ao tempo decorrido entre a inicialização e o encerramento do aplicativo.
- Clique em **Bloquear todo o acesso** para proibir uma conexão à Internet.
- Clique em **Conceder acesso de saída** para permitir uma conexão de saída (segurança **Rígida**).
- Clique em **Ajude-me a escolher** para exibir a Ajuda on-line sobre as permissões de acesso do aplicativo.

Alerta O aplicativo solicita acesso como servidor

Se você tiver selecionado a segurança **Rígida** nas opções de Configurações de segurança, o Personal Firewall exibirá um alerta (Figura 3-8) quando detectar que um aplicativo ao qual você concedeu acesso à Internet solicitou acesso como servidor.

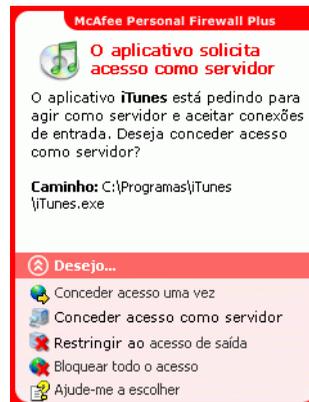



Figura 3-8. Alerta O aplicativo solicita acesso como servidor

Por exemplo, um alerta é exibido quando o MSN Messenger solicita acesso como servidor para enviar um arquivo durante um bate-papo.

Veja uma breve descrição do evento e escolha uma das opções a seguir:

- Clique em **Conceder acesso uma vez** para permitir ao aplicativo um acesso temporário à Internet. O acesso é limitado ao tempo decorrido entre a inicialização e o encerramento do aplicativo.
- Clique em **Conceder acesso como servidor** para permitir ao aplicativo uma conexão de entrada e saída da Internet.

- Clique em **Restringir ao acesso de saída** para proibir uma conexão de entrada da Internet.
- Clique em **Bloquear todo o acesso** para proibir uma conexão à Internet.
- Clique em **Ajude-me a escolher** para exibir a Ajuda on-line sobre os alertas verdes de permissões de acesso do aplicativo.

Alertas verdes

Os alertas verdes notificam sobre eventos no Personal Firewall, como aplicativos que receberam acesso à Internet automaticamente.

Programa com permissão para acessar a Internet — esse alerta é exibido quando o Personal Firewall concede acesso à Internet automaticamente a todos os aplicativos novos e, em seguida, o notifica (segurança **Confiável**). Um exemplo de aplicativo modificado é um aplicativo com regras modificadas para permitir automaticamente o acesso do aplicativo à Internet.

Alerta Aplicativo com permissão para acessar a Internet

Se você tiver selecionado a segurança **Confiável** nas opções de Configurações de segurança, o Personal Firewall concederá automaticamente acesso à Internet para todos os aplicativos novos e o notificará com um alerta (Figura 3-9).

Figura 3-9. Programa com permissão para acessar a Internet

Veja uma breve descrição do evento e escolha uma das opções a seguir:

- Clique em **Exibir o registro de aplicativos** para obter detalhes sobre o evento com o registro de Aplicativos da Internet (consulte *Sobre a página Aplicativos da Internet* na página 59 para obter detalhes).
- Clique em **Desativar este tipo de alerta** para impedir que esse tipo de alerta seja exibido.

- Clique em **Continuar o que eu estava fazendo** se não desejar executar nenhuma ação além do que o Personal Firewall já tenha feito.
- Clique em **Bloquear todo o acesso** para proibir uma conexão à Internet.

Alerta O aplicativo foi modificado

Se você tiver selecionado a segurança **Confiável** nas opções de Configurações de segurança, o Personal Firewall concederá automaticamente acesso à Internet a todos os aplicativos modificados. Veja uma breve descrição do evento e escolha uma das opções a seguir:

- Clique em **Exibir o registro de aplicativos** para obter detalhes sobre o evento com o registro de Aplicativos da Internet (consulte *Sobre a página Aplicativos da Internet* na página 59 para obter detalhes).
- Clique em **Desativar este tipo de alerta** para impedir que esse tipo de alerta seja exibido.
- Clique em **Continuar o que eu estava fazendo** se não desejar executar nenhuma ação além do que o Personal Firewall já tenha feito.
- Clique em **Bloquear todo o acesso** para proibir uma conexão à Internet.

Alertas azuis

Os alertas azuis contêm informações que não exigem respostas.

- **Tentativa de conexão bloqueada —** esse alerta é exibido quando o Personal Firewall bloqueia o tráfego não desejado da rede ou da Internet. (Segurança padrão, rígida ou confiável)

Alerta Tentativa de conexão bloqueada

Se você tiver selecionado a segurança **Confiável**, **Padrão** ou **Rígida**, o Personal Firewall exibirá um alerta (Figura 3-10) quando bloquear o tráfego não desejado da rede ou da Internet.

Figura 3-10. Alerta Tentativa de conexão bloqueada

Veja uma breve descrição do evento e escolha uma das opções a seguir:

- Clique em **Exibir o registro de eventos** para obter detalhes sobre o evento com o registro de Eventos de entrada do Personal Firewall (consulte *Sobre a página Eventos de entrada* na página 61 para obter detalhes).
- Clique em **Rastrear este endereço** para executar um rastreamento visual dos endereços IP deste evento.
- Clique em **Proibir este endereço** para impedir que o endereço acesse o seu computador. O endereço é adicionado à lista de endereços IP proibidos.
- Clique em **Confiar neste endereço** para permitir que o endereço IP acesse o seu computador.
- Clique em **Continuar o que eu estava fazendo** se não desejar executar nenhuma ação além do que o Personal Firewall já tenha feito.

McAfee Privacy Service 4

Bem-vindo ao McAfee Privacy Service.

O software McAfee Privacy Service oferece proteção avançada para você, sua família, seus dados pessoais e seu computador.

Recursos

Esta versão do McAfee Privacy Service oferece os seguintes recursos:

- Regras de utilização do horário na Internet - use uma grade de horários para especificar os dias e os horários em que os usuários podem acessar a Internet.
- Filtragem personalizada por palavras-chave - permite filtrar o acesso aos sites da Web com base em palavras-chave especificadas pelo administrador para certos níveis de faixas etárias.
- Backup e restauração do Privacy Service - permite salvar e restaurar as configurações do Privacy Service a qualquer momento.
- Bloqueador de Web bugs — bloqueia Web bugs (objetos obtidos em um site potencialmente mal-intencionado) para que eles não sejam carregados nas páginas navegadas da Web.
- Bloqueador de pop-ups — evita a exibição de janelas pop-up enquanto você navega na Internet.
- Shredder — o McAfee Shredder protege sua privacidade eliminando com segurança e rapidez arquivos indesejados.

O administrador

O administrador especifica quais usuários podem acessar a Internet, quando eles podem utilizá-la e o que eles podem fazer na Internet.

NOTA
Ele é considerado um adulto e, portanto, pode acessar todos os sites da Web, mas é solicitado a permitir ou proibir a transmissão de informações identificáveis como pessoais (PII) adicionais.

Assistente de configuração

O Assistente de configuração permite que você crie o administrador (se ainda não fez isso), gerencie configurações globais, insira informações pessoais e adicione usuários.

NOTA

Memorize sua senha de administrador e a resposta à pergunta de segurança para que possa efetuar logon no Privacy Service. Se você não conseguir efetuar logon, não poderá utilizar o Privacy Service e a Internet. Mantenha sua senha em segredo para que somente você possa alterar as configurações do Privacy Service.

Para que alguns sites da Web funcionem adequadamente, é necessário que os cookies estejam ativados.

O Privacy Service sempre aceita cookies da McAfee.com.

Recuperando a senha de administrador

Se você esquecer a senha de administrador, poderá acessá-la utilizando as informações de segurança digitadas durante a criação do perfil de administrador.

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **McAfee Privacy Service** e selecione **Conectar-se**.
2. Selecione **Administrador** no menu suspenso **Nome do usuário**.
3. Clique em **Esqueceu a senha?**
4. Insira a resposta à pergunta de segurança exibida e clique em **Obter senha**. É exibida uma mensagem contendo a sua senha. Se você esquecer a resposta à pergunta de segurança, desinstale o McAfee Privacy Service no modo de segurança (somente para Windows 2000 e Windows XP).

O usuário de inicialização

O usuário de inicialização é automaticamente conectado ao Privacy Service quando o computador é iniciado.

Por exemplo, se um usuário utilizar o computador ou a Internet com mais freqüência do que os outros, você poderá torná-lo o usuário de inicialização. Quando o usuário de inicialização utiliza o computador, ele não precisa conectar-se ao Privacy Service.

Se você tiver crianças, também poderá definir o mais novo como usuário de inicialização. Dessa forma, quando um usuário mais velho utilizar o computador, ele poderá efetuar o logoff da conta do usuário mais novo e efetuar o logon novamente utilizando seu próprio nome de usuário e senha. Isso protege os usuários mais novos contra sites da Web inadequados.

Abrindo o McAfee Privacy Service

Após a instalação do McAfee Privacy Service, o ícone da McAfee é exibido na bandeja de sistema do Windows, que fica localizada próximo ao relógio do sistema. O ícone da McAfee permite acessar o McAfee Privacy Service, o McAfee SecurityCenter e outros produtos McAfee instalados no computador.

Abrindo e conectando-se ao Privacy Service

Para abrir o Privacy Service:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **McAfee Privacy Service** e selecione **Conectar-se**.
2. Selecione seu nome de usuário no menu suspenso **Nome do usuário**.
3. Insira a senha no campo **Senha**.
4. Clique em **Conectar-se**.

Desativando o Privacy Service

Você deve efetuar logon no Privacy Service como administrador para desativá-lo.

Para desativar o Privacy Service:

Clique com o botão direito do mouse no ícone da McAfee , aponte para **McAfee Privacy Service** e selecione **Desconectar-se**.

NOTA
Se **Conectar-se** aparecer no lugar de **Desconectar-se**, é sinal de que você já está desconectado.

Atualizando o McAfee Privacy Service

O McAfee SecurityCenter verifica regularmente se há atualizações para o Privacy Service enquanto o computador está em execução e conectado à Internet. Se houver uma atualização disponível, o McAfee SecurityCenter solicitará que você atualize o Privacy Service.

Para verificar manualmente se existem atualizações, clique no ícone Atualizações localizado no painel superior.

Adicionando usuários

Para adicionar usuários, você deve conectar-se ao Privacy Service como administrador.

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows.
2. Aponte para **McAfee Privacy Service** e selecione **Gerenciar usuários**. Será exibida a caixa de diálogo **Selecionar usuário**.
3. Clique em **Adicionar** e insira o nome do novo usuário no campo **Nome do usuário**.

Definindo a senha

1. Digite uma senha no campo **Senha**. A senha pode conter até 50 caracteres, entre números e letras maiúsculas e minúsculas.
2. Digite a senha novamente no campo **Confirme a senha**.
3. Selecione **Fazer deste o usuário de inicialização** para que esse seja o usuário de inicialização.
4. Clique em **Avançar**.

Ao atribuir senhas, considere a faixa etária do usuário. Por exemplo, ao atribuir a senha de uma criança pequena, crie uma senha simples. Ao atribuir a senha de adolescentes ou adultos, crie senhas mais complexas.

Definindo a faixa etária

Selecione a configuração de faixa etária apropriada e clique em **Avançar**.

Definindo o bloqueador de cookies

Selecione a opção apropriada e clique em **Avançar**.

- **Rejeitar todos os cookies** — torna os cookies ilegíveis para os sites da Web que os enviaram. Para que alguns sites da Web funcionem adequadamente, é necessário ativar os cookies.
- **Perguntar ao usuário se ele aceitará cookies** — permite decidir se aceitará ou rejeitará cookies de acordo com cada caso. O Privacy Service informará quando o site da Web a ser exibido deseja enviar um cookie ao seu computador. Depois que você se decidir, não será mais perguntado sobre esse cookie novamente.
- **Aceitar todos os cookies** — permite que os sites da Web leiam os cookies que enviam ao seu computador.

NOTA
Para que alguns sites da Web funcionem adequadamente é necessário que os cookies estejam ativados.

O Privacy Service sempre aceita cookies da McAfee.

Definindo os limites de horário para uso da Internet

Para conceder uso irrestrito da Internet:

1. Selecione **Usar a Internet em qualquer horário**.
2. Clique em **Criar**. O novo usuário é exibido na lista Selecionar usuário.

Para conceder uso limitado da Internet:

1. Selecione **Restringir uso da Internet** e clique em **Editar**.
2. Na página Limites de horário para uso da Internet, percorra a grade de horários para selecionar o horário e o dia em que os usuários podem acessar a Internet.
   Você pode especificar os limites de horários em intervalos de trinta minutos. As partes verdes da grade são os períodos em que o usuário pode acessar a Internet. As partes vermelhas indicam quando o usuário não pode acessar a Internet. Se um usuário tentar utilizar a Internet quando não for permitido, o Privacy Service exibirá uma mensagem informando que o usuário não tem permissão para utilizar a Internet nesse horário. Para modificar os períodos em que o usuário pode acessar a Internet, percorra as partes verdes da grade.
3. Clique em **Concluído**.
4. Clique em **Criar**. O novo usuário é exibido na página Selecionar usuário. Se um usuário tentar utilizar a Internet quando não for permitido, o Privacy Service exibirá uma mensagem informando que o usuário não tem permissão para utilizar a Internet nesse horário.

Para proibir o uso da Internet:

- Selecione **Restringir uso da Internet** e clique em **Criar**. Quando o usuário usar o computador, ele será solicitado a conectar-se ao Privacy Service. Ele poderá utilizar o computador, mas não a Internet.

Editando usuários

Para editar usuários, você deve conectar-se ao Privacy Service como administrador.

Alterando senhas

1. Selecione o usuário cujas informações serão alteradas e clique em **Editar**.
2. Selecione **Senha** e insira a nova senha do usuário no campo **Nova senha**. A senha pode conter até 50 caracteres, entre números e letras maiúsculas e minúsculas.
3. Insira a mesma senha no campo **Confirme a senha** e clique em **Aplicar**.
4. Clique em **OK** na caixa de diálogo de confirmação.

NOTA
O administrador pode alterar a senha de um usuário sem saber a senha atual.

Alterando as informações de um usuário

1. Selecione o usuário cujas informações serão alteradas e clique em **Editar**.
2. Selecione **Informações do usuário**.
3. Insira o novo nome de usuário no campo **Novo nome de usuário**.
4. Clique em **Aplicar** e, em seguida, clique em **OK** na caixa de diálogo de confirmação.
5. Para restringir o acesso de um usuário aos sites da lista Sites da Web permitidos, selecione **Restringir o acesso deste usuário aos sites da Web que constam na lista "Sites da Web permitidos"**.

Alterando a configuração do bloqueador de cookies

1 Selecione o usuário cujas informações serão alteradas e clique em **Editar**.

2 Selecione **Cookies** e escolha a opção apropriada.

- **Rejeitar todos os cookies** — torna os cookies ilegíveis para os sites da Web que os enviaram. Para que alguns sites da Web funcionem adequadamente, é necessário ativar os cookies.
- **Perguntar ao usuário se ele aceitará cookies** — permite decidir se aceitará ou rejeitará cookies de acordo com cada caso. O Privacy Service informará quando o site da Web a ser exibido deseja enviar um cookie ao seu computador. Depois que você se decidir, não será mais perguntado sobre esse cookie novamente.
- **Aceitar todos os cookies** — permite que os sites da Web leiam os cookies que enviam ao seu computador.

3 Clique em **Aplicar** e, em seguida, clique em **OK** na caixa de diálogo de confirmação.

Editando a lista de cookies aceitos e rejeitados

1 Selecione **Perguntar ao usuário se ele aceitará cookies** e clique em **Editar** para especificar quais sites da Web têm permissão para ler cookies.

2 Especifique a lista que será modificada selecionando **Sites da Web que podem definir cookies** ou **Sites da Web que não podem definir cookies**.

3 No campo **http://**, insira o endereço do site da Web cujos cookies serão aceitos ou rejeitados.

4 Clique em **Adicionar**. O site será exibido na lista de sites da Web.

5 Clique em **Concluído** quando terminar de efetuar alterações.

NOTA
Para que alguns sites da Web funcionem adequadamente é necessário que os cookies estejam ativados.

O Privacy Service sempre aceita cookies da McAfee.

Alterando a faixa etária

1. Selecione o usuário cujas informações serão alteradas e clique em **Editar**.
2. Selecione **Faixa etária**.
3. Selecione uma nova faixa etária para o usuário e clique em **Aplicar**.
4. Clique em **OK** na caixa de diálogo de confirmação.

Alterando limites de horário para uso da Internet

1. Selecione o usuário cujas informações serão alteradas e clique em **Editar**.
2. Selecione **Limites de horário** e faça o seguinte:

Para permitir que o usuário utilize a Internet sempre:

1. Selecione **Usar a Internet em qualquer horário** e clique em **Aplicar**.
2. Clique em **OK** na caixa de diálogo de confirmação.

Para restringir o acesso do usuário à Internet:

1. Selecione **Restringir uso da Internet** e clique em **Editar**.
2. Na página Limites de horário para uso da Internet, selecione um quadrado verde ou vermelho e, em seguida, percorra a grade de horários para alterar os horários e os dias em que os usuários podem acessar a Internet atualmente. Você pode especificar os limites de horários em intervalos de trinta minutos. As partes verdes da grade são os períodos em que o usuário pode acessar a Internet. As partes vermelhas indicam quando o usuário não pode acessar a Internet. Se um usuário tentar utilizar a Internet quando não for permitido, o Privacy Service exibirá uma mensagem informando que o usuário não tem permissão para utilizar a Internet nesse horário.
3. Clique em **Aplicar**.
4. Na página Limites de horários, clique em **OK**.
5. Na caixa de diálogo de confirmação do McAfee Privacy Service, clique em **OK**.

Alterando o usuário de inicialização

1. Selecione o usuário que deseja designar como usuário de inicialização e clique em **Editar**.
2. Selecione **Informações do usuário**.
3. Selecione **Fazer deste o usuário de inicialização**.
4. Clique em **Aplicar** e, em seguida, clique em **OK** na caixa de diálogo de confirmação.

   NOTA
   Se já existir um usuário de inicialização, não será necessário desmarcá-lo.

Removendo usuários

1. Selecione o usuário a ser removido e clique em **Remover**.
2. Clique em **Sim** na caixa de diálogo de confirmação.
3. Feche a janela Privacy Service ao concluir as alterações.

Opções

Para configurar as opções do Privacy Service, é necessário conectar-se ao Privacy Service como administrador.

Bloqueando sites da Web

1. Clique em **Opções** e selecione **Lista de bloqueados**.
2. No campo **http://**, insira o URL do site da Web que deseja bloquear e clique em **Adicionar**. O site será exibido na lista **Sites da Web bloqueados**.

   NOTA
   Os usuários (incluindo os administradores) que pertencem ao nível Adulto podem acessar todos os sites da Web, mesmo que estes constem na lista Sites da Web bloqueados. Para testar os sites da Web bloqueados, os administradores devem fazer logon como usuários não-adultos.

Permitindo sites da Web

O administrador pode permitir que todos os usuários acessem determinados sites da Web. Essa opção se sobrepõe às configurações padrão do Privacy Service e aos sites da Web adicionados à lista de bloqueados.

1. Clique em **Opções** e selecione **Lista de permitidos**.
2. No campo **http://**, insira o URL do site da Web que será permitido e clique em **Adicionar**. O site será exibido na lista **Sites da Web permitidos**.

Bloqueando informações

O administrador pode impedir que outros usuários enviem informações pessoais específicas pela Internet (mas o administrador poderá enviar essas informações).

Quando o Privacy Service detecta informações identificáveis como pessoais (PII) em algo prestes a ser enviado, acontece o seguinte:

- Se você for um administrador, será avisado e poderá decidir se enviará ou não as informações.
- Se o usuário conectado não for o administrador, as informações bloqueadas serão substituídas por *MFEMFEMFE*. Por exemplo, se você enviar o e-mail *Lance Armstrong ganha tour* e Armstrong estiver definido como informação pessoal a ser bloqueada, o e-mail enviado será *Lance MFEMFEMFE ganha tour*.

Adicionando informações

1. Clique em **Opções** e selecione **Bloquear informações**.
2. Clique em **Adicionar**. O menu suspenso **Selecionar tipo** será exibido.
3. Selecione o tipo de informações a serem bloqueadas.
4. Insira as informações nos campos apropriados e clique em **OK**. As informações inseridas serão exibidas na lista.

Editando informações

1. Clique em **Opções** e selecione **Bloquear informações**.
2. Selecione as informações a serem editadas e clique em **Editar**.
3. Faça as alterações apropriadas e clique em **OK**. Se não for necessário alterar as informações, clique em **Cancelar**.

Removendo informações pessoais

1. Clique em **Opções** e selecione **Bloquear informações**.
2. Selecione as informações a serem removidas e clique em **Remover**.
3. Clique em **Sim** na caixa de diálogo de confirmação.

Bloqueando Web bugs

Os Web bugs são pequenos arquivos gráficos que podem enviar mensagens a terceiros, incluindo o rastreamento de seus hábitos de navegação na Internet ou a transmissão de informações pessoais a um banco de dados externo. As pessoas que recebem os Web bugs podem usar essas informações para criar perfis de usuário.

Para evitar que os Web bugs sejam carregados em páginas navegadas na Web, selecione **Bloquear Web Bugs neste computador**.

Bloqueando anúncios

Geralmente, os anúncios são gráficos transmitidos por um domínio de terceiros a uma página da Web ou janela pop-up. O Privacy Service não bloqueia os anúncios fornecidos pelo mesmo domínio da página da Web do host.

Pop-ups são janelas secundárias do navegador que apresentam anúncios indesejados, exibidos automaticamente quando você visita um site da Web. O Privacy Service bloqueia somente os pop-ups exibidos automaticamente quando uma página da Web é carregada. O Privacy Service não bloqueia pop-ups iniciados com um clique em um link. Para exibir um pop-up bloqueado, mantenha a tecla CTRL pressionada e atualize a página da Web.

Configure o Privacy Service para bloquear anúncios e pop-ups quando você estiver utilizando a Internet.

1. Clique em **Opções** e selecione **Bloquear anúncios**.
2. Selecione a opção apropriada.
   - **Bloquear anúncios neste computador** — bloqueia anúncios enquanto você estiver utilizando a Internet.
   - **Bloquear pop-ups neste computador** — bloqueia pop-ups enquanto você estiver utilizando a Internet.
3. Clique em **Aplicar** e, em seguida, clique em **OK** na caixa de diálogo de confirmação.

Para desativar o bloqueio de pop-ups, clique com o botão direito do mouse na página da Web, aponte para **Bloqueador de pop-ups da McAfee** e cancele a seleção **Ativar bloqueador de pop-ups**.

Permitindo cookies de sites da Web específicos

Se você bloquear cookies ou pedir para ser avisado antes que eles sejam aceitos e perceber que determinados sites da Web não funcionam adequadamente, configure o Privacy Service para permitir que o site leia cookies.

1. Clique em **Opções** e selecione **Cookies**.
2. No campo **http://**, insira o endereço do site da Web que precisa ler os cookies e clique em **Adicionar**. O endereço será exibido na lista **Aceitar cookies de sites da Web**.

Registro de eventos

Para exibir o registro de eventos, é necessário conectar-se ao Privacy Service como administrador. Depois, selecione **Registro de eventos** e clique em qualquer entrada de registro para exibir seus detalhes. Para salvar ou exibir um registro salvo, selecione a guia Registros salvos.

Data e hora

Por padrão, o registro de eventos exibe as informações em ordem cronológica, com os eventos mais recentes na parte superior. Se as entradas do registro de eventos não estiverem em ordem cronológica, clique no título Data e hora.

A data é exibida no formato mês/dia/ano e a hora no formato 6:00/18:00, por exemplo.

Usuário

O usuário é a pessoa que estava conectada e usando a Internet quando o Privacy Service registrou o evento.

Resumo

Os resumos exibem uma descrição concisa e breve do que o Privacy Service está fazendo para proteger os usuários e do que os usuários estão fazendo na Internet.

Detalhes do evento

O campo Detalhes do evento exibe detalhes da entrada.

Salvando o registro atual

A página Registro atual exibe informações sobre as últimas ações administrativas e dos usuários. Essas informações podem ser salvas para serem exibidas posteriormente.

Para salvar o registro de eventos atual

1. Conecte-se ao Privacy Service como administrador.
2. Selecione **Registro de eventos**.
3. Na página Registro atual, clique em **Salvar registro**.
4. No campo **Nome do arquivo**, digite o nome do arquivo de registro.
5. Clique em **Salvar**.

Exibindo registros salvos

A página Registro atual exibe informações sobre as últimas ações administrativas e dos usuários. Essas informações podem ser salvas para serem exibidas posteriormente.

Para exibir um registro salvo

1. Conecte-se ao Privacy Service como administrador.
2. Selecione **Registro de eventos**.
3. Na página Registro atual, clique em **Abrir registro**.
4. Na caixa de diálogo **Selecione o registro salvo que será exibido**, selecione o arquivo de backup do banco de dados e clique em **Abrir**.

Utilitários

Para acessar os utilitários, conecte-se ao Privacy Service como administrador e clique em **Utilitários**.

Para remover arquivos, pastas ou todo o conteúdo de um disco, clique em **McAfee Shredder**. Para salvar as configurações do banco de dados do Privacy Service, clique em **Backup**. Para restaurar as suas configurações, clique em **Restaurar**.

Apagando arquivos permanentemente com o McAfee Shredder

O McAfee Shredder protege sua privacidade eliminando, com segurança e rapidez, arquivos indesejados.

Os arquivos excluídos podem ser recuperados em seu computador até mesmo depois do esvaziamento da Lixeira. Quando um arquivo é excluído, o Windows simplesmente marca esse espaço na unidade de disco para indicar que ele não está mais sendo utilizado, mas o arquivo continua presente.

Por que o Windows deixa vestígios do arquivo?

Para excluir um arquivo permanentemente, é preciso sobrescrever várias vezes o arquivo existente com novos dados. Se o Microsoft Windows excluísse os arquivos com segurança, cada operação de arquivo seria muito lenta. A destruição de um documento nem sempre impede que ele seja recuperado, pois alguns programas fazem cópias ocultas temporárias de documentos abertos. Se você destruiu apenas os documentos exibidos no Explorer, ainda pode haver cópias temporárias desses documentos. Recomendamos que você destrua periodicamente o espaço livre na unidade de disco para garantir que as cópias temporárias sejam excluídas permanentemente.

NOTA
Com ferramentas legais de computador, registros de impostos, currículos ou outros documentos excluídos podem ser recuperados.

O que o McAfee Shredder apaga

O McAfee Shredder permite apagar permanentemente e com segurança:

- Um ou mais arquivos ou pastas
- Um disco inteiro
- Os rastros deixados pela navegação na Web

Apagando arquivos permanentemente no Windows Explorer

Para destruir um arquivo pelo Windows Explorer:

1. Abra o Windows Explorer e selecione os arquivos a serem destruídos.
2. Clique com o botão direito do mouse no item selecionado, aponte para **Enviar para** e selecione **McAfee Shredder**.

Esvaziando a Lixeira do Windows

Se os arquivos estiverem na Lixeira, o McAfee Shredder oferecerá um método mais seguro para esvaziá-la.

Para destruir o conteúdo da Lixeira:

1 Na área de trabalho do Windows, clique com o botão direito do mouse na Lixeira.

2 Selecione **Destruir a Lixeira** e siga as instruções da tela.

Personalizando as configurações do Shredder

Você pode:

- Especificar o número de destruições.
- Mostrar uma mensagem de aviso ao destruir arquivos.
- Verificar se há erros no disco rígido antes de destruir.
- Adicionar o McAfee Shredder ao menu Enviar para.
- Colocar um ícone do Shredder na área de trabalho do Windows.

Para personalizar as configurações do Shredder, abra o McAfee Shredder, clique em **Propriedades** e siga as instruções da tela.

Fazendo backup do banco de dados do Privacy Service

É possível restaurar o banco de dados do Privacy Service de duas maneiras. Se o banco de dados estiver corrompido ou tiver sido excluído, o Privacy Service solicitará a restauração do banco de dados do Privacy Service. Também é possível restaurar as configurações do banco de dados durante a execução do Privacy Service.

1 Clique em **Utilitários** e selecione **Backup**.

2 Clique em **Procurar** para selecionar um local para o arquivo de banco de dados e, em seguida, clique em **OK**.

3 Digite uma senha no campo **Senha**.

4 Insira novamente a senha no campo **Confirme a senha** e clique em **Backup**.

5 Clique em **OK** na caixa de diálogo de confirmação.

6 Feche a janela do Privacy Service ao terminar.

NOTA
Mantenha essa senha em segredo e procure não esquecê-la. Sem a senha, não será possível restaurar as configurações do Privacy Service.

Restaurando o banco de dados de backup

1 O Privacy Service oferece duas maneiras de restaurar as configurações originais:

- Carregar o arquivo do banco de dados depois que o Privacy Service solicitar a restauração das configurações porque o banco de dados está corrompido ou foi excluído.
- Carregar o arquivo de backup do banco de dados durante a execução do Privacy Service.

Para restaurar as configurações do Privacy Service quando solicitado:

1 Clique em **Procurar** para localizar o arquivo.

2 Digite a senha no campo **Senha**.

3 Clique em **Restaurar**.
Se você não fez backup do banco de dados do Privacy Service, esqueceu a senha de backup ou a restauração do banco de dados não está funcionando, remova e reinstale o Privacy Service.

Para restaurar as configurações durante a execução do Privacy Service:

1 Clique na guia **Utilitários**.

2 Clique em **Restaurar**.

3 Clique em **Procurar** e digite o caminho e o nome do arquivo de backup.

4 Clique em **Abrir**.

5 Digite a senha no campo **Senha**.

6 Clique em **Restaurar** e, em seguida, clique em **OK** na caixa de diálogo de confirmação do McAfee Privacy Service.

Opções do usuário

Essas instruções não se aplicam ao administrador.

Você pode alterar sua senha e o nome de usuário. Recomendamos alterar a senha após o administrador fornecê-la. Recomendamos também alterá-la uma vez por mês ou se suspeitar que alguém a conhece. Isso ajudará a evitar que outras pessoas utilizem a Internet com seu nome de usuário.

Alterando a senha

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **McAfee Privacy Service** e selecione **Opções**.
2. Clique em **Senha** e digite a senha antiga no campo **Senha antiga**.
3. Digite a nova senha no campo **Nova senha**.
4. Digite a nova senha novamente no campo **Confirme a senha** e clique em **Aplicar**.
5. Clique em **OK** na caixa de diálogo de confirmação. Agora você tem uma nova senha.

Alterando o nome de usuário

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **McAfee Privacy Service** e selecione **Opções**.
2. Clique em **Informações do usuário**.
3. Digite o novo nome de usuário no campo **Novo nome de usuário** e clique em **Aplicar**.
4. Clique em **OK** na caixa de diálogo de confirmação. Agora você tem um novo nome de usuário.

Limpando o cache

Recomendamos a limpeza do cache para evitar que crianças acessem as páginas da Web visitadas recentemente. Para limpar o cache, faça o seguinte:

1. Abra o Internet Explorer.
2. No menu **Ferramentas**, clique em **Opções da Internet**. Será exibida a caixa de diálogo Opções da Internet.
3. Na seção **Arquivos de Internet temporários**, clique em **Excluir arquivos**. Será exibida a caixa de diálogo Excluir arquivos.
4. Selecione **Excluir todo o conteúdo off-line** e clique em **OK**.
5. Clique em **OK** para fechar a caixa de diálogo Opções da Internet.

Aceitando cookies

Essa opção estará disponível somente se o administrador permitir aceitar ou rejeitar os cookies interceptados.

Se você acessar sites da Web que exijam cookies, poderá permitir que esses sites leiam cookies.

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **McAfee Privacy Service** e selecione **Opções**.
2. Clique em **Cookies aceitos**.
3. Insira o URL do site da Web no campo **http://** e clique em **Adicionar**. O site será exibido na lista **Sites da Web**.

Se for necessário remover um site da Web da lista:

1. Selecione o URL do site na lista **Sites da Web**.
2. Clique em **Remover** e, depois, clique em **Sim** na caixa de diálogo de confirmação.

Rejeitando cookies

Essa opção estará disponível somente se o administrador permitir aceitar ou rejeitar os cookies interceptados.

Se você acessar sites da Web que não exijam cookies, poderá rejeitar os cookies sem ser avisado.

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **McAfee Privacy Service** e selecione **Opções**.
2. Clique em **Cookies rejeitados**.
3. Insira o URL do site no campo **http://** e clique em **Adicionar**. O site será exibido na lista **Sites da Web**.

Se for necessário remover um site da Web da lista:

1. Selecione o URL do site na lista **Sites da Web**.
2. Clique em **Remover** e, depois, clique em **Sim** na caixa de diálogo de confirmação.

McAfee SpamKiller 5

Bem-vindo ao McAfee SpamKiller.

O software McAfee SpamKiller ajuda a impedir que spams entrem em sua caixa de entrada de e-mail. Ele oferece os seguintes recursos:

Recursos

Esta versão do SpamKiller oferece os seguintes recursos:

- Filtragem - as opções avançadas de filtragem oferecem novas técnicas, incluindo suporte à filtragem de metacaracteres e à identificação de texto de lixo eletrônico
- Phishing – o plug-in AntiPhishing do navegador, na barra de ferramentas do Internet Explorer, identifica e bloqueia sites da Web de phishing em potencial.
- Integração com o Microsoft Outlook e o Outlook Express – a barra de ferramentas fornece uma pasta, no cliente de e-mail, para bloquear o spam diretamente.
- Instalação - instalação e configuração simplificadas. A detecção automática da conta garante a facilidade na instalação e na configuração, e a integração com as contas de e-mail existentes.
- Atualizações - as atualizações automáticas são executadas silenciosamente em segundo plano, sempre vigilantes para minimizar a exposição às novas ameaças de spam.
- Interface - interface de usuário intuitiva, para manter o computador livre de spam.
- Suporte - suporte técnico gratuito com troca de mensagens instantâneas e e-mail ao vivo, para assistência imediata, fácil e personalizada ao cliente.

Processamento da mensagem de spam - por padrão, as mensagens de spam são marcadas como [SPAM] e colocadas na pasta do SpamKiller no Outlook e no Outlook Express ou na caixa de entrada. As mensagens marcadas também são exibidas na página E-mail aceito.

Opções do usuário

- Bloquear spams utilizando filtros e colocar spams em quarentena fora da caixa de entrada
- Exibir mensagens bloqueadas e aceitas
- Monitorar e filtrar várias contas de e-mail
- Importar endereços de amigos para a Lista de amigos
- Revidar contra remetentes de spam (relatar spam, reclamar de spam, criar filtros personalizados)
- Impedir que crianças vejam mensagens de spam
- Bloqueio de clique único e recuperação de clique único
- Suporte a conjunto de caracteres de dois bytes
- Suporte multiusuário (para Windows 2000 e Windows XP).

Filtragem

- Atualizar filtros automaticamente
- Criar filtros personalizados para bloquear e-mails que contenham, basicamente, imagens, texto invisível ou formatação inválida
- Mecanismo de filtragem central em várias camadas
- Filtro contra ataques de dicionários
- Filtragem adaptável em vários níveis
- Filtros de segurança

Noções básicas sobre o painel superior

Os ícones a seguir são exibidos no painel superior de cada página do SpamKiller:

- Clique em **Alternar usuário** para efetuar logon como outro usuário.

  Nota: A opção **Alternar usuário** estará disponível somente se o computador estiver executando o Windows 2000 ou o Windows XP, se vários usuários tiverem sido adicionados ao SpamKiller e se você estiver conectado ao SpamKiller como administrador.

- Clique em **Suporte** para abrir a página de suporte online da McAfee, que fornece tópicos atuais sobre o SpamKiller e outros produtos da McAfee, respostas para perguntas freqüentes e muito mais. É necessário estar conectado à Internet para acessar a página Suporte.

- Clique em **Ajuda** para abrir a Ajuda online, que fornece instruções detalhadas sobre como configurar e usar o SpamKiller.

Após a instalação do SpamKiller, o ícone da McAfee é exibido na bandeja do sistema, próxima ao relógio do sistema. O ícone da McAfee permite acessar o SpamKiller, o McAfee SecurityCenter e outros produtos McAfee instalados no seu computador.

Desativando o SpamKiller

Você pode desativar o SpamKiller e impedir a filtragem de emails.

Para desativar a filtragem:

Clique com o botão direito do mouse no ícone da McAfee , aponte para **SpamKiller** e, em seguida, clique em **Desativar**. Ou clique na guia **Resumo** e, em seguida, em **Clique aqui para desativar**.

Para ativar a filtragem:

Clique com o botão direito do mouse no ícone da McAfee, aponte para **SpamKiller** e, em seguida, clique em **Ativar**. Ou clique na guia **Resumo** e, em seguida, em **Clique aqui para ativar**.

Noções básicas sobre a página Resumo

Clique na guia **Resumo** para abrir a página Resumo (Figura 5-11).

- **Visão geral do status do SpamKiller**- indica se a filtragem está ativada, quando uma Lista de amigos foi atualizada pela última vez e o número de mensagens de spam recebidas hoje. Aqui é possível desativar ou ativar a filtragem do SpamKiller, atualizar Listas de amigos e abrir a página E-mail bloqueado.
- **E-mails mais recentes que foram identificados como spam e bloqueados** - as últimas mensagens de spam que o SpamKiller bloqueou (removidas da Caixa de entrada).
- **Visão geral dos e-mails** - exibe o número total de e-mails, spams (mensagens bloqueadas) e a porcentagem do total de spams recebidos.
- **Spam recente** - uma análise do tipo de spam recebido nos últimos 30 dias.

Figura 5-11. página Resumo

Integração ao Microsoft Outlook e ao Outlook Express

Você pode usar os principais recursos do SpamKiller diretamente no Outlook Express 6.0, no Outlook 98, no Outlook 2000 e no Outlook XP, selecionando o menu ou a barra de ferramentas do SpamKiller.

A barra de ferramentas do SpamKiller é exibida à direita das barras de ferramentas padrão do Outlook e do Outlook Express. Se ela não estiver visível, expanda a janela do aplicativo de e-mail ou clique nas setas para exibir mais barras de ferramentas.

Quando a barra de ferramentas do SpamKiller for exibida pela primeira vez no aplicativo de e-mail, você poderá usar os comandos da barra de ferramentas somente em mensagens novas. Os e-mails de spam existentes devem ser excluídos manualmente.

Gerenciando contas de e-mail e usuários

Esta seção descreve como gerenciar contas e usuários.

Adicionando contas de e-mail

Você pode adicionar as seguintes contas de e-mail:

- Conta de e-mail padrão (POP3) - a maioria dos usuários domésticos utiliza esse tipo de conta.
- Conta MSN/Hotmail - contas MSN/Hotmail baseadas na Web.

NOTA
Se o computador executa o Windows 2000 ou o Windows XP e você pretende adicionar vários usuários ao SpamKiller, adicione os usuários primeiro para poder adicionar as contas de e-mail aos respectivos perfis. Para obter mais informações, consulte *Adicionando usuários* na página 111. Se você adicionar vários usuários ao SpamKiller, a conta será adicionada ao perfil do usuário que estiver conectado ao SpamKiller no momento.

Para adicionar uma conta de e-mail:

1 Clique na guia **Configurações** para abrir a página Configurações (Figura 5-12) e, em seguida, clique em **Contas de e-mail**. A caixa de diálogo **Contas de e-mail** é exibida e mostra todas as contas adicionadas ao SpamKiller.

    NOTA
    Se vários usuários tiverem sido adicionados ao SpamKiller, a lista exibirá as contas de e-mail do usuário que estiver conectado ao SpamKiller no momento.

2 Clique em **Adicionar**. O Assistente de contas de e-mail é exibido.

    Siga as instruções nas caixas de diálogo exibidas.

Se você adicionar uma conta MSN/Hotmail, o SpamKiller procurará uma lista de endereços MSN/Hotmail que será importada para a Lista de amigos pessoais.

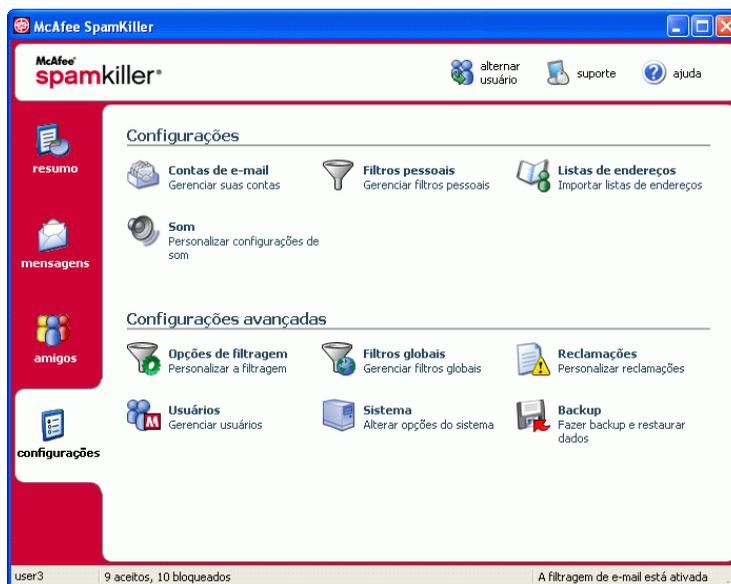



Figura 5-12. página Configurações

Indicando seu cliente de e-mail para o SpamKiller

Se você adicionar uma conta que o SpamKiller não conseguir detectar (a conta não aparece na caixa de diálogo **Selecionar conta**) ou se você quiser ler o e-mail MSN/Hotmail como uma conta POP3 no SpamKiller, indique o cliente de e-mail para o SpamKiller, alterando o servidor de e-mails recebidos.

Por exemplo, se o servidor de e-mails recebidos for “mail.mcafee.com”, altere-o para “localhost”.

Excluindo contas de e-mail

Exclua uma conta de e-mail do SpamKiller caso não queira mais que ele a filtre.

Excluindo uma conta de e-mail do SpamKiller

1 Clique na guia **Configurações** e, em seguida, selecione **Contas de e-mail**. A caixa de diálogo **Contas de e-mail** é exibida e mostra todas as contas adicionadas ao SpamKiller.

   NOTA
   Se vários usuários tiverem sido adicionados ao SpamKiller, a lista exibirá as contas de e-mail do usuário que estiver conectado ao SpamKiller no momento.

2 Selecione uma conta e, em seguida, clique em **Excluir**.

Editando propriedades da conta de e-mail

É possível editar informações sobre uma conta de e-mail adicionada ao SpamKiller. Por exemplo, altere o endereço de e-mail, a descrição da conta, as informações do servidor, a freqüência com que o SpamKiller verifica se há spam na conta e como o computador se conecta à Internet.

Contas POP3

Editando contas POP3

1 Clique na guia **Configurações** e, em seguida, clique em **Contas de e-mail**. A caixa de diálogo **Contas de e-mail** é exibida e mostra todas as contas adicionadas ao SpamKiller.

   NOTA
   Se vários usuários tiverem sido adicionados ao SpamKiller, a lista exibirá as contas de e-mail do usuário que estiver conectado ao SpamKiller no momento.

2 Selecione uma conta POP3 e, em seguida, clique em **Editar**.

3 Clique na guia **Geral** para editar a descrição da conta e o endereço de e-mail.

   - **Descrição** - descrição da conta. Digite qualquer informação nessa caixa.
   - **Endereço de e-mail** - endereço de e-mail da conta.

4 Clique na guia **Servidores** para editar as informações do servidor.

- **E-mails recebidos** - nome do servidor que recebe e-mails.
- **Nome do usuário** - nome de usuário usado para acessar a conta. Conhecido também como nome de conta.
- **Senha** - senha usada para acessar a conta.
- **E-mails enviados** - nome do servidor que envia e-mails. Clique em **Mais** para editar os requisitos de autenticação do servidor de saída.

5 Clique na guia **Verificando** para editar a freqüência com que o SpamKiller deve verificar se há spam na conta:

a Selecione **Verificar a cada** ou **Verificar diariamente às** e, em seguida, digite uma hora na caixa correspondente. Se você digitar o número zero, o SpamKiller verificará a conta apenas ao se conectar.

b Selecione períodos adicionais para o SpamKiller filtrar a conta:

Verificar ao iniciar - se você tem uma conexão direta e quer que o SpamKiller verifique a conta sempre que o computador for iniciado.

Verificar quando uma conexão for discada - se você tem uma conexão discada e quer que o SpamKiller verifique a conta sempre que você se conectar à Internet.

6 Clique na guia **Conexão** para especificar como o SpamKiller discará uma conexão da Internet para verificar se há novas mensagens a serem filtradas na caixa de entrada.

- **Nunca discar uma conexão** - o SpamKiller não disca automaticamente uma conexão para você. Primeiro, é necessário iniciar manualmente a conexão discada.
- **Discar quando necessário** - uma conexão não está disponível e o SpamKiller tenta se conectar automaticamente usando a conexão de Internet discada padrão.
- **Discar sempre** - o SpamKiller tenta se conectar automaticamente usando a conexão discada que você especificou.
- **Permanecer conectado após a filtragem** - o computador permanece conectado à Internet após o término da filtragem.

7 Clique na guia **Avançado** para editar opções avançadas.

- **Deixar as mensagens de spam no servidor** - se desejar que cópias das mensagens bloqueadas permaneçam no servidor de e-mail. Você pode ver o e-mail no cliente de e-mail e na página E-mail bloqueado do SpamKiller. Se a caixa de seleção não estiver marcada, as mensagens bloqueadas serão exibidas somente na página E-mail bloqueado.
- **Porta POP3** - (número da porta POP3) o servidor POP3 cuida das mensagens recebidas.
- **Porta SMTP** - (número da porta SMTP) o servidor SMTP cuida das mensagens enviadas.
- **Tempo limite do servidor** - período máximo que o SpamKiller espera para receber e-mails antes de parar.

  Aumente o valor do tempo limite do servidor se houver problemas em receber mensagens. Se a sua conexão de e-mail estiver lenta, o aumento do valor do tempo limite do servidor permitirá que o SpamKiller aguarde um pouco mais antes de atingir o tempo limite.

8 Clique em **OK**.

Contas MSN/Hotmail

Editando contas MSN/Hotmail

1 Clique na guia **Configurações** e, em seguida, clique em **Contas de e-mail**.

A caixa de diálogo **Contas de e-mail** é exibida com todas as contas de e-mail adicionadas ao SpamKiller.

> **NOTA**
> Se vários usuários tiverem sido adicionados ao SpamKiller, a lista exibirá as contas de e-mail do usuário que estiver conectado ao SpamKiller no momento.

2 Selecione uma conta MSN/Hotmail e clique em **Editar**.

3 Clique na guia **Geral** para editar a descrição da conta e o endereço de e-mail.

- **Descrição** - descrição da conta. Digite qualquer informação nessa caixa.
- **Endereço de e-mail** - endereço de e-mail da conta.

4 Clique na guia **Servidores** para editar as informações do servidor.

- **E-mails recebidos** - nome do servidor que recebe e-mails.
- **Senha** - senha usada para acessar a conta.
- **E-mails enviados** - nome do servidor que envia e-mails.

- **Usar um servidor SMTP para o envio de e-mails** - para enviar mensagens de erro sem incluir a linha de assinatura MSN na mensagem de erro. A linha de assinatura MSN permite que os remetentes de spam reconheçam facilmente se a mensagem de erro é falsa.

  Clique em **Mais** para alterar os requisitos de autenticação do servidor de saída.

5 Clique na guia **Verificação** para especificar a freqüência com que o SpamKiller deve verificar se há spam na conta:

   a Selecione **Verificar a cada** ou **Verificar diariamente às** e, em seguida, digite uma hora na caixa correspondente. Se você digitar o número zero, o SpamKiller verificará a conta apenas ao se conectar.

   b Selecione períodos adicionais para o SpamKiller filtrar a conta:

   Verificar ao iniciar - selecione esta opção se você tem uma conexão direta e quer que o SpamKiller verifique a conta sempre que o computador for iniciado.

   Verificar quando uma conexão for discada - selecione esta opção se você tem uma conexão discada e quer que o SpamKiller verifique a conta sempre que você se conectar à Internet.

6 Clique na guia **Conexão** para especificar como o SpamKiller discará uma conexão da Internet para verificar se há novas mensagens a serem filtradas na caixa de entrada.

- **Nunca discar uma conexão** - o SpamKiller não disca automaticamente uma conexão para você. Primeiro, é necessário iniciar manualmente a conexão discada.
- **Discar quando necessário** - quando uma conexão da Internet não está disponível, o SpamKiller tenta se conectar automaticamente usando a conexão de Internet discada padrão.
- **Discar sempre** - o SpamKiller tenta se conectar automaticamente usando a conexão discada que você especificou.
- **Permanecer conectado após a filtragem** - o computador permanece conectado à Internet após o término da filtragem.

7 Clique em **OK**.

Configurando uma conta Hotmail para bloquear spams no Outlook ou no Outlook Express

O SpamKiller pode filtrar contas Hotmail diretamente. Consulte os detalhes na ajuda online. Porém, só é possível bloquear mensagens ou adicionar amigos usando a barra de ferramentas do SpamKiller no Outlook ou no Outlook Express após a configuração da conta Hotmail.

1. Configure sua conta Hotmail no MSK.
2. Se você tiver uma conta Hotmail existente no Outlook ou no Outlook Express, remova-a primeiro.
3. Adicione a conta Hotmail ao Outlook ou ao Outlook Express. Verifique se você selecionou **POP3** como tipo de conta e tipo de servidor de e-mails recebidos.
4. Nomeie o servidor de entrada como `localhost`.
5. Digite o nome do servidor SMTP de saída disponível (necessário).
6. Conclua o processo de configuração da conta. Agora você pode bloquear os novos e-mails de spam do Hotmail ou adicionar um amigo.

Contas MAPI

As condições a seguir são necessárias para a integração com êxito do SpamKiller ao MAPI no Outlook:

- Somente para Outlook 98, o Outlook ser inicialmente instalado com o suporte corporativo/de grupo de trabalho.
- Somente para Outlook 98, a primeira conta de e-mail ser uma conta MAPI.
- O computador estar conectado ao domínio.

Editando contas MAPI

1. Clique na guia **Configurações** e, em seguida, clique em **Contas de e-mail**. A caixa de diálogo **Contas de e-mail** é exibida e mostra todas as contas adicionadas ao SpamKiller.

   NOTA
   Se vários usuários tiverem sido adicionados ao SpamKiller, a lista exibirá as contas de e-mail do usuário que estiver conectado ao SpamKiller no momento.

2. Selecione uma conta MAPI e, em seguida, clique em **Editar**.
3. Clique na guia **Geral** para editar a descrição da conta e o endereço de e-mail.
   - **Descrição** - descrição da conta. Digite qualquer informação nessa caixa.
   - **Endereço de e-mail** - endereço de e-mail da conta.

4 Clique na guia **Perfil** para editar as informações do perfil.

- **Perfil** - perfil MAPI da conta.
- **Senha** - senha que corresponde ao perfil MAPI, se configurado (não é necessariamente a senha da conta de e-mail).

5 Clique na guia **Conexão** para especificar como o SpamKiller discará uma conexão da Internet para verificar se há novas mensagens a serem filtradas na caixa de entrada:

- **Nunca discar uma conexão** - o SpamKiller não disca automaticamente uma conexão para você. Primeiro, é necessário iniciar manualmente a conexão discada.
- **Discar quando necessário** - quando uma conexão da Internet não está disponível, o SpamKiller tenta se conectar automaticamente usando a conexão de Internet discada padrão.
- **Discar sempre** - o SpamKiller tenta se conectar automaticamente usando a conexão discada que você especificou.
- **Permanecer conectado após a filtragem** - o computador permanece conectado à Internet após o término da filtragem.

6 Clique em **OK**.

Adicionando usuários

O SpamKiller pode configurar vários usuários, correspondentes aos usuários configurados no sistema operacional Windows 2000 ou Windows XP.

Quando o SpamKiller é instalado no seu computador, um perfil de usuário de administrador é automaticamente criado para o usuário do Windows que efetuou logon. Se você adicionar contas de e-mail ao SpamKiller durante a instalação, essas contas serão adicionadas ao perfil de usuário do administrador.

Antes de adicionar mais contas de e-mail ao SpamKiller, determine se precisa adicionar mais usuários. A adição de usuários é vantajosa se várias pessoas usarem o computador e tiverem suas próprias contas de e-mail. A conta de e-mail de cada usuário é adicionada ao perfil correspondente, permitindo que os usuários gerenciem suas próprias contas de e-mail, configurações pessoais, filtros pessoais e a Lista de amigos pessoais.

Os tipos de usuário definem as tarefas que um usuário pode executar no SpamKiller. A tabela a seguir é um resumo das permissões para cada tipo de usuário. Os administradores podem executar todas as tarefas, enquanto os usuários limitados só podem executar tarefas de acordo com os seus perfis pessoais. Por exemplo, os administradores podem ver todo o conteúdo das mensagens bloqueadas, enquanto os usuários limitados podem ver apenas a linha do assunto.

Tarefas	Administrador	Usuário limitado
Gerenciar contas de e-mail pessoais, filtros pessoais, Lista de amigos pessoais e configurações de som pessoais.	X	X
Gerenciar as páginas pessoais E-mail bloqueado e E-mail aceito	X	X
Exibir o texto das mensagens bloqueadas	X	
Exibir o texto das mensagens aceitas	X	X
Gerenciar os filtros globais e a Lista de amigos globais	X	
Relatar spams à McAfee	X	X
Enviar reclamações e mensagens de erro	X	X
Gerenciar reclamações e mensagens de erro (criar, editar e excluir modelos de mensagem)	X	
Gerenciar usuários (criar, editar e remover usuários)	X	
Fazer backup e restaurar o SpamKiller	X	
Exibir a página Resumo do spam recebido	X	X

Quando um usuário efetua logon no computador após ser adicionado, ele é solicitado a adicionar uma conta de e-mail ao respectivo perfil de usuário.

Para adicionar e gerenciar usuários, é exigido o seguinte:

- É necessário estar conectado ao SpamKiller como administrador.
- Você deve ter o Windows 2000 ou o Windows XP no seu computador.
- Os usuários adicionados ou gerenciados devem ter contas de usuário do Windows.

Senhas de usuário e proteção de crianças contra spams

A criação de uma senha de usuário fortalece o nível de privacidade. As configurações pessoais, a lista de amigos e a lista de -mails aceitos de um usuário não podem ser acessadas por outro usuário sem a senha de logon. A criação de senhas também é benéfica para impedir que crianças acessem o SpamKiller e vejam o conteúdo das mensagens de spam.

Criando uma senha para um usuário do SpamKiller

1. Clique na guia **Configurações** e, em seguida, clique em **Usuários**.
2. Selecione um usuário e clique em **Editar**.
3. Digite uma senha na caixa **Senha**. Quando o usuário acessar o SpamKiller, ele precisará usar a senha para efetuar logon.

   IMPORTANTE
   Se você esquecer a senha, não poderá recuperá-la. Somente um administrador do SpamKiller poderá criar uma nova senha para você.

Adicionando um usuário ao SpamKiller

1. Clique na guia **Configurações** e, em seguida, clique em **Usuários**.
2. Clique em **Adicionar**.

   Uma lista de usuários do Windows é exibida. Para adicionar um usuário que não aparece na lista, crie uma conta de usuário do Windows para essa pessoa. Em seguida, o novo usuário deverá efetuar logon no computador pelo menos uma vez. Depois disso, adicione o usuário ao SpamKiller.

   NOTA
   Os usuários do Windows com direitos de administrador também possuem esses direitos no SpamKiller.

3. Selecione o usuário a ser adicionado e clique em **OK**. O usuário é adicionado ao SpamKiller e seu nome é exibido na lista de usuários do SpamKiller.
4. Clique em **Fechar** quando terminar de adicionar usuários.

Para criar a senha de um usuário, consulte *Criando uma senha para um usuário do SpamKiller* na página 112.

Na próxima vez que o usuário efetuar logon no seu computador, ele será solicitado a adicionar uma conta de e-mail ao respectivo perfil de usuário do SpamKiller. Você pode adicionar contas de e-mail ao perfil do usuário se estiver conectado ao SpamKiller como o próprio usuário e possuir as informações necessárias sobre a conta de e-mail. Para obter detalhes, consulte *Adicionando contas de e-mail* na página 103.

Editando um perfil de usuário do SpamKiller

1. Clique na guia **Configurações** e, em seguida, clique em **Usuários**. Uma lista de usuários do SpamKiller é exibida.
2. Selecione um usuário e clique em **Editar**.
3. Digite um novo nome e uma nova senha.

Excluindo um perfil de usuário do SpamKiller

AVISO
Quando um perfil de usuário é removido, também são removidas as contas de e-mail desse usuário no SpamKiller.

1. Clique na guia **Configurações** e, em seguida, clique em **Usuários**. Uma lista de usuários do SpamKiller é exibida.
2. Selecione um usuário da lista e clique em **Excluir**.

Efetuando logon no SpamKiller em um ambiente multiusuário

Quando os usuários efetuam logon no computador e abrem o SpamKiller, eles são conectados automaticamente ao programa nos respectivos perfis de usuário. Se os usuários tiverem senhas do SpamKiller atribuídas, eles precisarão digitá-las na caixa de diálogo **Efetuar logon**.

Alternando usuários

É necessário estar conectado ao SpamKiller como administrador.

1. Clique em **Alternar usuário** na parte superior da página. A caixa de diálogo **Alternar usuário** é exibida.
2. Selecione um usuário e clique em **OK**. Se o usuário possuir uma senha, a caixa de diálogo **Efetuar logon** é exibida. Digite a senha de usuário na caixa **Senha** e clique em **OK**.

Usando a Lista de amigos

Recomendamos que você adicione os nomes e endereços de e-mail dos seus amigos à Lista de amigos. O SpamKiller não bloqueia as mensagens das pessoas dessa lista; portanto, a inclusão de amigos na lista ajuda a garantir o recebimento de mensagens legítimas.

O SpamKiller permite adicionar nomes, endereços de e-mail, domínios e listas de mala direta às Listas de amigos. É possível adicionar um endereço de cada vez ou todos de uma vez, importando uma lista de endereços do programa de e-mail.

O SpamKiller mantém dois tipos de lista:

- **Lista de amigos globais** - afeta todas as contas de e-mail de todos os usuários do SpamKiller. Se diversos usuários foram adicionados, é necessário estar conectado ao SpamKiller como administrador para gerenciar a lista.
- **Lista de amigos pessoais** - afeta todas as contas de e-mail associadas a um usuário específico. Se diversos usuários foram adicionados, é necessário estar conectado ao SpamKiller como o usuário para gerenciar a lista.

Você pode adicionar amigos a uma Lista de amigos para garantir que os respectivos e-mails não sejam bloqueados. A página Amigos mostra os nomes e endereços que foram adicionados à Lista de amigos. A página também mostra a data em que o amigo foi adicionado e o número total de mensagens recebidas desse amigo.

Clique na guia **Endereços de e-mail** para ver endereços de e-mail da Lista de amigos. Clique na guia **Domínios** para exibir os endereços de domínio da lista. Clique na guia **Listas de mala direta** para ver listas de mala direta da Lista de amigos.

Para alternar entre a Lista de amigos globais e a Lista de amigos pessoais, clique na seta para baixo localizada na guia **Endereço de e-mail**, **Domínios** ou **Listas de mala direta** e, em seguida, selecione **Lista de amigos pessoais**.

Abrindo uma Lista de amigos

1 Para abrir uma Lista de amigos, clique na guia **Amigos**. A página Amigos é exibida (Figura 5-13).

2 Clique na guia **Endereço de e-mail**, **Domínios** ou **Lista de mala direta**. A Lista de amigos globais é exibida. Para ver sua Lista de amigos pessoais, clique na seta para baixo em uma das guias e, em seguida, selecione **Lista de amigos pessoais**.

NOTA
Se o computador estiver executando o Windows 2000 ou o Windows XP e vários usuários tiverem sido adicionados ao SpamKiller, alguns usuários limitados poderão ver apenas a respectiva Lista de amigos pessoais.

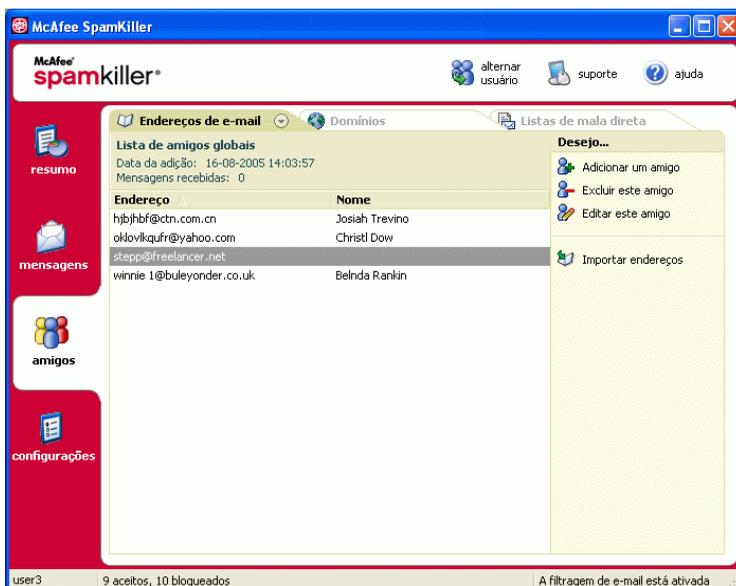



Figura 5-13. página Amigos

Importando listas de endereços

Importe listas de endereços para uma Lista de amigos de modo manual ou automático. A importação automática permite que o SpamKiller verifique regularmente se há novos endereços nas listas de endereços e importe-os automaticamente para uma Lista de amigos.

Você pode importar listas de endereços por meio dos seguintes programas de e-mail:

- Microsoft Outlook (98 e posterior)
- Microsoft Outlook Express (todas as versões)
- Netscape Communicator (versão 6 e versões anteriores, se exportadas como arquivo LDIF)
- Qualcomm Eudora (versão 5 e posterior)
- IncrediMail Xe
- MSN/Hotmail
- Qualquer programa capaz de exportar a lista de endereços como arquivo de texto simples

Importando uma lista de endereços automaticamente

Você pode atualizar sua Lista de amigos pessoais regularmente criando uma programação para importar os endereços de listas de endereços.

1. Clique na guia **Configurações** e, em seguida, clique em **Listas de endereços**. A caixa de diálogo **Importar listas de endereços** é exibida, mostrando uma relação das listas de endereços que o SpamKiller verifica regularmente e das quais importa os endereços novos.
2. Clique em **Adicionar**. A caixa de diálogo **Importar programação** é exibida.
3. Selecione o **Tipo** de lista de endereços a ser importada e a **Origem** da lista.
4. Na caixa **Programação**, selecione a freqüência com que o SpamKiller deve verificar se há novos endereços na lista de endereços.
5. Clique em **OK**. Após a atualização, os novos endereços são exibidos na Lista de amigos pessoais.

Importando uma lista de endereços manualmente:

Você pode importar listas de endereços manualmente para a Lista de amigos pessoais ou para a Lista de amigos globais.

> **NOTA**
> Se o computador estiver executando o Windows 2000 ou o Windows XP e vários usuários tiverem sido adicionados ao SpamKiller, você deverá estar conectado como administrador para adicionar amigos à Lista de amigos globais.

1 Clique na guia **Amigos** e, em seguida, clique em **Importar lista de endereços**.

   A caixa de diálogo **Importar lista de endereços** é exibida, mostrando uma relação dos tipos de lista de endereços que podem ser importadas.

2 Selecione um tipo de lista de endereços a ser importada ou clique em **Procurar** para importar os endereços armazenados em um arquivo.

   Para importar a lista de endereços somente para a Lista de amigos pessoais, verifique se a caixa de seleção **Adicionar à Lista de amigos pessoais** está marcada. Para importar a lista de endereços somente para a Lista de amigos globais, verifique se a caixa de seleção não está marcada.

3 Clique em **Avançar**. Uma página de confirmação exibirá o número de endereços que o SpamKiller adicionou.

4 Clique em **Concluir**. Os endereços são exibidos na Lista de amigos globais ou na Lista de amigos pessoais.

Editando informações sobre a lista de endereços

Edite informações de uma lista de endereços importada automaticamente.

1 Clique na guia **Configurações** e, em seguida, clique em **Listas de endereços**.

2 Selecione uma lista de endereços e clique em **Editar**.

3 Edite as informações sobre a lista de endereços e clique em **OK**.

Excluindo uma lista de endereços da Lista de importação automática

Remova uma entrada da lista de endereços quando não quiser mais que o SpamKiller importe automaticamente endereços dessa lista.

1 Clique na guia **Configurações** e, em seguida, clique em **Listas de endereços**.

2 Selecione uma lista de endereços e, em seguida, clique em **Excluir**. É exibida uma caixa de diálogo de confirmação.

3 Clique em **Sim** para remover a lista de endereços da lista.

Adicionando amigos

Para assegurar que todos os e-mails recebidos são de amigos, adicione os respectivos nomes e endereços a uma Lista de amigos. Você pode adicionar amigos das páginas Amigos, E-mail bloqueado e E-mail aceito; e os amigos contidos no Microsoft Outlook ou no Outlook Express.

NOTA
Se o computador estiver executando o Windows 2000 ou o Windows XP e vários usuários tiverem sido adicionados ao SpamKiller, você deverá estar conectado como administrador para adicionar amigos à Lista de amigos globais.

Adicionando amigos da página E-mail bloqueado ou E-mail aceito

1. Clique na guia **Mensagens** e, em seguida, clique na guia **E-mail bloqueado** ou **E-mail aceito**.

   Ou

   No menu do SpamKiller no Microsoft Outlook ou no Outlook Express, selecione **Exibir mensagens bloqueadas** para exibir a página E-mail bloqueado referente a essa conta.

   A página E-mail bloqueado ou E-mail aceito é exibida.

2. Selecione uma mensagem de um remetente que deseja adicionar a uma Lista de amigos e clique em **Adicionar um amigo**.

3. Na caixa **Endereço**, digite o endereço a ser adicionado à Lista de amigos. A caixa **Endereço** talvez já contenha o endereço da mensagem selecionada.

4. Digite o nome do seu amigo na caixa **Nome**.

5. Na caixa **Tipo de amigo**, selecione o tipo de endereço a ser adicionado.

   - **Endereço de e-mail único** - o endereço de e-mail do remetente é adicionado à seção Domínios da Lista de amigos.
   - **Todos no domínio** - o nome de domínio é adicionado à seção **Domínios**, na Lista de amigos. O SpamKiller aceita todos os e-mails provenientes do domínio.
   - **Lista de mala direta** - o endereço é adicionado à seção **Lista de mala direta** da Lista de amigos.

   Para adicionar o endereço somente à Lista de amigos pessoais, verifique se a caixa de seleção **Adicionar à Lista de amigos pessoais** está marcada. Para adicionar o endereço somente à Lista de amigos globais, verifique se a caixa de seleção não está marcada.

6. Clique em **OK**. Todas as mensagens desse amigo são marcadas, indicando que foram enviadas por um amigo, e são exibidas na página E-mail aceito.

Adicionando amigos da página Amigos

1. Clique na guia **Amigos** e, em seguida, clique em **Adicionar um amigo**. A caixa de diálogo **Propriedades do amigo** é exibida.
2. Na caixa **Endereço**, digite o endereço a ser adicionado à Lista de amigos.
3. Digite o nome do seu amigo na caixa **Nome**.
4. Na caixa **Tipo de amigo**, selecione o tipo de endereço a ser adicionado.
   - **Endereço de e-mail único** - o endereço de e-mail do remetente é adicionado à seção Domínios da Lista de amigos.
   - **Todos no domínio** - o nome de domínio é adicionado à seção **Domínios** da Lista de amigos. O SpamKiller aceita todos os e-mails provenientes do domínio.
   - **Lista de mala direta** - o endereço é adicionado à seção **Lista de mala direta** da Lista de amigos.

   Para adicionar o endereço somente à Lista de amigos pessoais, verifique se a caixa de seleção **Adicionar à Lista de amigos pessoais** está marcada. Para adicionar o endereço somente à Lista de amigos globais, verifique se a caixa de seleção não está marcada.
5. Clique em **OK**. Todas as mensagens desse amigo são marcadas, indicando que foram enviadas por um amigo e são exibidas na página E-mail aceito.

Adicionando amigos do Microsoft Outlook

1. Abra sua conta de e-mail no Microsoft Outlook ou no Outlook Express.
2. Selecione uma mensagem cujo remetente será adicionado a uma Lista de amigos.
3. Clique em na barra de ferramentas do Microsoft Outlook. Todas as mensagens desse amigo são marcadas, indicando que foram enviadas por um amigo, e são exibidas na página E-mail aceito.

Editando amigos

1 Clique na guia **Amigos** e, em seguida, clique na guia **Endereços de e-mail**, **Domínios** ou **Listas de mala direta**.

   A Lista de amigos globais é exibida. Para ver sua Lista de amigos pessoais, clique na seta para baixo em uma das guias e, em seguida, selecione **Lista de amigos pessoais**.

   NOTA
   Se o computador estiver executando o Windows 2000 ou o Windows XP e vários usuários tiverem sido adicionados ao SpamKiller, somente os administradores poderão acessar a Lista de amigos globais.

2 Selecione um endereço na lista e clique em **Editar**.

3 Edite as informações apropriadas e clique em **OK**.

Excluindo amigos

Remova os endereços que não deseja mais em uma Lista de amigos.

1 Clique na guia **Amigos** e, em seguida, clique na guia **Endereços de e-mail**, **Domínios** ou **Listas de mala direta**.

   A Lista de amigos globais é exibida. Para ver sua Lista de amigos pessoais, clique na seta para baixo em uma das guias e, em seguida, selecione **Lista de amigos pessoais**.

   NOTA
   Se o computador estiver executando o Windows 2000 ou o Windows XP e vários usuários tiverem sido adicionados ao SpamKiller, somente os administradores poderão acessar a Lista de amigos globais.

2 Selecione um endereço da lista e clique em **Excluir um amigo**. É exibida uma caixa de diálogo de confirmação.

3 Clique em **Sim** para excluir o amigo.

Trabalhando com mensagens bloqueadas e aceitas

Clique na guia **Mensagens** para abrir a página Mensagens (Figura 5-14) e acessar as suas mensagens bloqueadas e aceitas. As páginas E-mail bloqueado e E-mail aceito possuem recursos semelhantes.

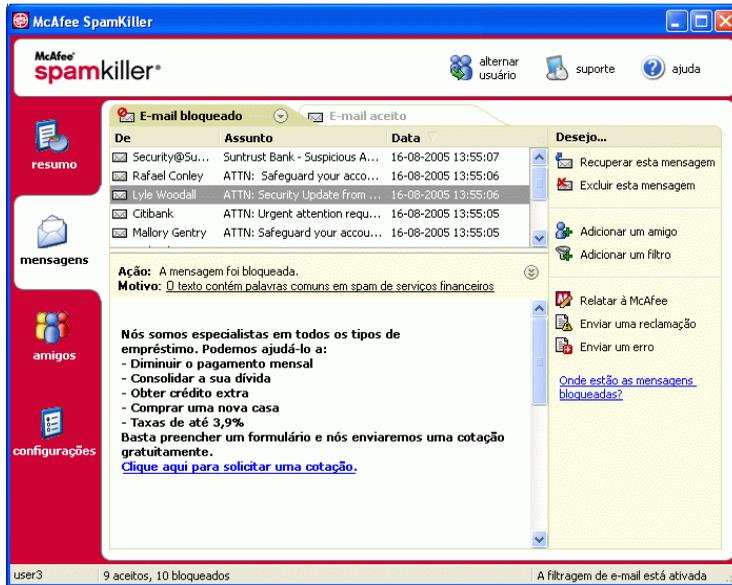



Figura 5-14. página Mensagens

Página E-mail bloqueado

Clique na guia **E-mail bloqueado** na página Mensagens para exibir as mensagens bloqueadas.

> **NOTA**
> Também é possível acessar as mensagens bloqueadas no Microsoft Outlook, selecionando o menu do SpamKiller e, em seguida, clicando em **Exibir mensagens bloqueadas**.

As mensagens bloqueadas são mensagens que o SpamKiller identificou como spam, removeu da caixa de entrada e colocou na página E-mail bloqueado.

A página E-mail bloqueado exibe todas as mensagens de spam removidas das contas de e-mail. Para exibir os e-mails bloqueados de uma conta específica, clique na seta para baixo localizada na guia **E-mail bloqueado** e selecione a conta a ser exibida.

O painel de mensagens superior lista as mensagens de spam classificadas por data. A mensagem mais recente é exibida primeiro. O painel de visualização inferior contém o texto da mensagem selecionada.

NOTA
Se o computador estiver executando o Windows 2000 ou o Windows XP, vários usuários foram adicionados ao SpamKiller e você estiver conectado ao SpamKiller como usuário limitado, o conteúdo da mensagem não será exibido no painel de visualização inferior.

O painel do meio exibe os detalhes da mensagem. Clique nas setas para baixo até expandir o painel de detalhes e exibir o texto e os cabeçalhos da mensagem em formato nativo, inclusive as marcas de formatação HTML. O painel de detalhes da mensagem exibe as informações a seguir.

- **Ação** - como o SpamKiller processou a mensagem de spam. A ação está associada à ação do filtro que bloqueou a mensagem.
- **Razão** - por que o SpamKiller bloqueou a mensagem. Você pode clicar na razão para abrir o editor de filtros e exibir o filtro. O editor de filtros exibe o que o filtro procura em uma mensagem e a ação executada pelo SpamKiller com as mensagens encontradas pelo filtro.
- **De** - o remetente da mensagem.
- **Data** - a data em que a mensagem foi enviada para você.
- **Para** - para quem a mensagem foi enviada.
- **Assunto** - o tópico que aparece na linha de assunto da mensagem.

A coluna da esquerda contém ícones ao lado das mensagens, caso tenham sido enviadas reclamações manuais ou mensagens de erro.

- Reclamação enviada - foi enviada uma reclamação sobre a mensagem.
- Mensagem de erro enviada - uma mensagem de erro foi enviada para o endereço de resposta da mensagem de spam.
- Reclamação e mensagens de erro enviadas - uma reclamação e uma mensagem de erro foram enviadas.

Para obter mais informações sobre o local onde estão as mensagens bloqueadas, consulte *Onde estão as mensagens bloqueadas* na página 126.

Página E-mail aceito

Clique na guia **E-mail aceito** na página Mensagens para exibir as mensagens aceitas.

A página E-mail aceito exibe todas as mensagens da caixa de entrada em todas as contas de e-mail. Entretanto, para contas MAPI, a página E-mail aceito não contém e-mail interno. Para exibir os e-mails aceitos de uma conta específica, clique na seta para baixo da guia **E-mail aceito** e selecione uma conta a ser exibida.

> **NOTA**
> O SpamKiller foi projetado para aceitar e-mails legítimos. Entretanto, se forem exibidos e-mails legítimos na lista E-mail bloqueado, você poderá colocá-los de volta na caixa de entrada (e na lista E-mail aceito) selecionando-os e clicando em **Recuperar esta mensagem**.

Da mesma forma que a página E-mail bloqueado, o painel de mensagens superior lista mensagens classificadas por data. O painel de visualização inferior contém o texto da mensagem selecionada.

O painel do meio explica se a mensagem foi enviada por alguém de uma Lista de amigos ou se a mensagem está de acordo com os critérios de um filtro, mas a ação do filtro foi definida como **Aceitar** ou **Marcar como possível spam**. Clique nas setas para baixo para expandir o painel de detalhes e exibir o texto e os cabeçalhos da mensagem em formato nativo, inclusive as marcas de formatação HTML.

O painel de detalhes da mensagem exibe o seguinte:

- **Ação** - como o SpamKiller processou a mensagem.
- **Razão** - se alguma mensagem foi marcada, essa opção explica por que o SpamKiller marcou a mensagem.
- **De** - o remetente da mensagem.
- **Data** - a data em que a mensagem foi enviada para você.
- **Para** - para quem a mensagem foi enviada.
- **Assunto** - o tópico que aparece na linha de assunto da mensagem.

Um dos ícones a seguir aparece ao lado de uma mensagem.

- E-mail de um amigo - o SpamKiller detectou que o remetente da mensagem consta em uma Lista de amigos. É uma das mensagens que você deseja guardar.
- Possível spam - a mensagem corresponde a um filtro com uma ação definida como Marcar como possível spam.
- Reclamação enviada - uma reclamação sobre a mensagem foi enviada.

- Mensagem de erro enviada - uma mensagem de erro foi enviada para o endereço de resposta na mensagem de spam.
- Reclamação e mensagens de erro enviadas - uma reclamação e uma mensagem de erro foram enviadas.

Tarefas das páginas E-mail bloqueado e E-mail aceito

O painel à direita nas páginas E-mail bloqueado e E-mail aceito lista as tarefas que você pode executar.

- **Bloquear esta mensagem** - remove uma mensagem da caixa de entrada e a coloca na página E-mails bloqueados do SpamKiller. (Esta opção é exibida somente na página E-mail aceito.)
- **Recuperar esta mensagem** - coloca uma mensagem de volta na caixa de entrada (opção exibida somente na página E-mail bloqueado) e abre a caixa de diálogo **Opções de resgate**. Você pode adicionar automaticamente o remetente à sua lista de Amigos e resgatar todas as mensagens do remetente.
- **Excluir esta mensagem** - remove uma mensagem selecionada.
- **Adicionar um amigo** - adiciona o nome, o endereço de e-mail, o domínio ou uma lista de mala direta do remetente a uma Lista de amigos.
- **Adicionar um filtro** - cria um filtro.
- **Relatar à McAfee** - informa a McAfee sobre as mensagens de spam que você recebeu.
- **Enviar uma reclamação** - envia uma reclamação sobre spams ao administrador do domínio do remetente ou a outro endereço de e-mail que você digitar.
- **Enviar um erro** - envia uma mensagem de erro ao endereço de resposta de uma mensagem de spam.

Recuperando mensagens

Se a página E-mail bloqueado ou a pasta do SpamKiller no Microsoft Outlook e Outlook Express contiverem e-mails legítimos, você poderá colocar as mensagens de volta na sua caixa de entrada.

Na página E-mail bloqueado

1 Clique na guia **Mensagens** e, em seguida, clique na guia **E-mail bloqueado**.

   Ou

   No menu do SpamKiller no Microsoft Outlook ou no Outlook Express, selecione **Exibir mensagens bloqueadas** para exibir a página E-mail bloqueado referente a essa conta.

2 Selecione uma mensagem e clique em **Recuperar esta mensagem** . A caixa de diálogo **Opções de resgate** é exibida.

   - **Adicionar amigo** - adiciona o remetente à Lista de amigos.
   - **Recuperar todas do mesmo remetente** - recupera todas as mensagens bloqueadas do remetente da mensagem selecionada.

3 Clique em **OK**. A mensagem é colocada de volta na caixa de entrada e na página E-mail aceito.

Na pasta do SpamKiller no Microsoft Outlook ou no Outlook Express

Selecione as mensagens e clique em **Recuperar seleção** no menu do SpamKiller ou na barra de tarefas. A sua seleção é colocada de volta na Caixa de entrada e a marca da mensagem ([SPAM] por padrão) é removida.

Bloqueando mensagens

Bloqueie as mensagens de spam que estão na caixa de entrada. Quando você bloqueia uma mensagem, o SpamKiller cria automaticamente um filtro para removê-la da caixa de entrada. Você pode bloquear mensagens da caixa de entrada na página E-mail aceito, ou no Microsoft Outlook ou no Outlook Express.

Na página E-mail aceito

1. Clique na guia **Mensagens** e, em seguida, clique na guia **E-mail aceito**. A página E-mail aceito é exibida com as mensagens existentes na caixa de entrada.

2. Selecione uma mensagem e, em seguida, clique em **Bloquear esta mensagem**. Ela é removida da Caixa de entrada e da página E-mail aceito. Uma cópia da mensagem aparece na página E-mail bloqueado.

No Microsoft Outlook

No Microsoft Outlook, as mensagens dos membros de um servidor do Exchange são consideradas seguras e não são filtradas pelo SpamKiller. Apenas as mensagens de fontes externas são filtradas.

1. Abra a caixa de entrada do Microsoft Outlook ou Outlook Express.

2. Selecione uma mensagem e clique em . Uma cópia da mensagem é colocada na página E-mail bloqueado.

Onde estão as mensagens bloqueadas

Por padrão, as mensagens de spam são marcadas como [SPAM] e colocadas na pasta do SpamKiller no Outlook e no Outlook Express, ou na caixa de entrada. As mensagens marcadas também são exibidas na página E-mail aceito.

Excluindo uma mensagem manualmente

1. Clique na guia **Mensagens** e, em seguida, clique na guia **E-mail bloqueado**.

   Ou

   No menu do SpamKiller no Microsoft Outlook ou no Outlook Express, selecione **Exibir mensagens bloqueadas** para exibir a página E-mail bloqueado referente a essa conta.

2. Selecione uma mensagem a ser excluída.

3. Clique em **Excluir esta mensagem**. A caixa de diálogo de confirmação é exibida.

4. Clique em **Sim** para excluir a mensagem.

Modificando o modo como as mensagens de spam são processadas

Quando o spam é encontrado, a mensagem é marcada ou bloqueada. As mensagens de spam são removidas do servidor a cada vez que o SpamKiller se conecta a ele.

Marcação

A linha de assunto do e-mail é marcada com [SPAM] e a mensagem vai para a caixa de entrada ou para a pasta do SpamKiller, caso seja utilizado o Microsoft Outlook ou o Outlook Express.

Bloqueando

A mensagem é removida e colocada na pasta E-mail bloqueado do SpamKiller. Quando e-mails legítimos são bloqueados, é possível recuperar a mensagem (consulte Recuperando mensagens).

O SpamKiller remove automaticamente as mensagens bloqueadas da página E-mail bloqueado após 15 dias. Você pode alterar a freqüência com que as mensagens bloqueadas são removidas.

O SpamKiller não remove automaticamente as mensagens da página E-mail aceito, pois esta reflete as mensagens que estão na Caixa de entrada.

Modificando o modo como o SpamKiller processa mensagens de spam

1 Clique na guia **Configurações** e, em seguida, no ícone **Opções de filtragem**.

2 Clique na guia **Processamento**.

- **Colocar o spam na caixa de e-mail bloqueado** - as mensagens de spam são removidas da caixa de entrada e colocadas na página E-mail bloqueado do SpamKiller.

- **Marcar spam e manter na caixa de entrada** - é a configuração padrão. As mensagens de spam permanecem na caixa de entrada, mas a linha de assunto da mensagem inclui [SPAM].

  Manter o e-mail bloqueado por ____ dias - as mensagens bloqueadas permanecem na página E-mail bloqueado durante o período que você especificar.

  Manter o e-mail aceito por ____ dias - as mensagens aceitas permanecem na página E-mail aceito durante o período que você especificar.

3 Clique em **OK**.

Usando o filtro AntiPhishing

O e-mail não solicitado é classificado como spam (e-mails que solicitam que você adquira algo) ou phishing (e-mails que solicitam que você forneça informações pessoais para um site da Web enganoso, conhecido ou em potencial).

O filtro AntiPhishing da McAfee o ajuda a proteger-se contra sites da Web que estão na lista negra (de phishing confirmado ou sites enganosos associados) e na lista cinza (podem apresentar conteúdo perigoso ou links para sites da lista negra).

Ao navegar em um site enganoso (conhecido ou potencial), você será direcionado à página do filtro AntiPhishing da McAfee.

Para alterar as configurações do AntiPhishing, siga estas etapas:

1 Abra o Internet Explorer.

2 No menu **Ferramentas**, selecione **Filtro AntiPhishing da McAfee**.

- **Ativar a filtragem do site da Web** - ativado por padrão. Para desativar a filtragem AntiPhishing, desmarque essa caixa de seleção.
- **Permitir o acesso a sites da Web na lista negra** - coloca um link na página de redirecionamento aos sites da lista negra. Ao clicar neste link, você é levado ao site da Web.
- **Permitir o acesso a sites da Web na lista cinza** - coloca um link na página de redirecionamento aos sites da lista cinza. Ao clicar neste link, você é levado ao site da Web.

3 Ao terminar, clique em **OK**.

Adicionando amigos a uma Lista de amigos

Consulte *Adicionando amigos da página E-mail bloqueado ou E-mail aceito* na página 118.

Adicionando filtros

Para obter mais informações sobre filtros, consulte *Trabalhando com filtros* na Ajuda online.

1 Para criar um filtro global, clique na guia **Configurações**, selecione **Filtros globais** e, em seguida, clique em **Adicionar**.

   Ou

   Para criar um Filtro pessoal, clique na guia **Configurações**, selecione **Filtros pessoais** e, em seguida, clique em **Adicionar**.

   Ou

   Clique na guia **Mensagens** e na guia **E-mail bloqueado** ou **E-mail aceito** e selecione **Adicionar um filtro**.

2 Clique em **Adicionar** para começar a criar uma condição de filtro. A caixa de diálogo **Condição do filtro** é exibida.

3 Crie uma condição de filtro seguindo estas etapas.

   A condição do filtro é uma instrução que informa ao SpamKiller o que ele deve procurar em uma mensagem. No exemplo “O texto da mensagem contém hipoteca”, o SpamKiller procura mensagens com a palavra “hipoteca”. Para obter mais informações, consulte *Condições de filtro* na Ajuda online.

   a Selecione um tipo de condição na primeira caixa.

   b Selecione ou digite valores nas caixas subseqüentes.

   c Se as opções a seguir forem exibidas, selecione-as para definir ainda mais a condição do filtro.

      Procurar também nos códigos de formatação - essa opção é exibida somente se a condição do filtro for definida para pesquisar o texto da mensagem. Quando essa caixa de seleção está marcada, o SpamKiller procura a expressão indicada no texto e nos códigos de formatação da mensagem.

      Comparar variações - permite que o SpamKiller detecte erros ortográficos comuns cometidos intencionalmente pelos remetentes de spam. Por exemplo, a palavra “comum” pode ser escrita incorretamente como “c0mum” para escapar dos filtros.

      Expressões regulares (RegEx) - permite especificar padrões de caracteres usados nas condições de filtro. Para testar um padrão de caracteres, clique em **Testar RegEx**.

      Sensível a maiúsculas e minúsculas - essa opção é exibida somente para condições em que um valor de condição seja digitado. Com essa caixa de seleção marcada, o SpamKiller diferencia maiúsculas e minúsculas no valor digitado.

   d Clique em **OK**.

4 Crie outra condição de filtro da maneira especificada a seguir ou vá para a Etapa 5 e selecione uma ação de filtro.

   a Clique em **Adicionar** e crie a condição de filtro. Clique em **OK** quando terminar de criar a condição de filtro.

      As duas condições aparecem na lista de Condições de filtro, associadas por **e**. O **e** indica que o SpamKiller procura mensagens que correspondam às *duas* condições de filtro Se desejar que o SpamKiller procure mensagens que correspondam a uma das duas condições, substitua o **e** por **ou** clicando em **e** e selecionando **ou** na caixa apresentada.

   b Clique em **Adicionar** para criar outra condição ou vá para a Etapa 5 e selecione uma ação de filtro.

      Se você criou um total de três ou mais condições do filtro, poderá agrupá-las para criar cláusulas. Para obter exemplos de agrupamento, consulte *Agrupando filtros* na Ajuda online.

      Para agrupar condições do filtro, selecione uma condição e clique em **Agrupar**. Para desagrupar condições do filtro, selecione uma condição agrupada e clique em **Desagrupar**.

5 Selecione uma ação do filtro na caixa **Ação**. A ação do filtro informa ao SpamKiller como processar mensagens encontradas por esse filtro. Para obter mais informações, consulte *Ações de filtro* na Ajuda online.

6 Clique em **Avançado** para selecionar as opções avançadas de filtro (a seleção das opções avançadas não é obrigatória). Para obter mais informações, consulte *Opções avançadas de filtro* na Ajuda online.

7 Clique em **OK** quando terminar de criar o filtro.

   NOTA
   Para editar uma condição, selecione-a e clique em **Editar**.
   Para excluir uma condição, selecione-a e clique em **Excluir**.

Expressões regulares

As expressões regulares estão disponíveis apenas para as seguintes condições de filtro: **O assunto**, **O texto da mensagem**, **Pelo menos uma das seguintes frases**.

Esses caracteres e seqüências especiais podem ser usados como expressões regulares para definir as condições de filtro Por exemplo:

- A expressão regular **[0-9]*\.[0-9]+** corresponde a números de ponto flutuante fornecidos na notação que não é de engenharia. A expressão regular corresponde a: “12.12”, “.1212” e “12.0”, mas não a “12” e “12”.
- A expressão regular **\D*[0-9]+\D*** corresponde a todas as palavras com números: “SpamKi11er” e V1AGRA”, mas não “SpamKiller” e “VIAGRA”.

****

Marca o próximo caractere como especial ou literal. Por exemplo, “n““corresponde ao caractere “n“. “\n“corresponde ao caractere de nova linha. A seqüência “\\“corresponde a “\“ e “\(“corresponde a “(“.

^

Corresponde ao início da entrada.

$

Corresponde ao final da entrada.

*****

Corresponde ao caractere precedente, zero ou mais vezes. Por exemplo, “zo*“ corresponde a “z“ ou “zoo“.

+

Corresponde ao caractere precedente, uma ou mais vezes. Por exemplo, “zo+“ corresponde a “zoo“, mas não a “z“.

?

Corresponde ao caractere precedente, zero ou uma vez. Por exemplo, “a?ve?“ corresponde ao “ve“ de “never“.

.

Corresponde a qualquer caractere único, exceto o de nova linha.

(padrão)

Corresponde ao padrão e lembra a correspondência. A subseqüência de caracteres correspondente pode ser recuperada da coleção resultante de correspondências, usando o item [0]...[n]. Para corresponder aos caracteres de parênteses ( ), use “\(“ ou “\)“.

x|y

Corresponde a x ou y. Por exemplo, “z|wood“ corresponde a “z“ ou “wood“. “(z|w)oo“corresponde a “zoo“ ou “wood“.

{n}

O n é um número inteiro não-negativo. Corresponde exatamente a n vezes. Por exemplo, “o{2}“ não corresponde ao “o“ de “Bob,“ mas corresponde aos dois primeiros "o" de “foooood“.

{n,}

O n é um número inteiro não-negativo. Corresponde a no mínimo n vezes. Por exemplo, “o{2,}“ não corresponde ao “o“ de “Bob“ e corresponde a todos “o“ de “foooood“. “o{1,}“ equivale a “o+“. “o{0,}“ equivale a “o*“.

{n,m}

O m e n são números inteiros não-negativos. Correspondem a no mínimo n e no máximo m vezes. Por exemplo, “o{1,3}“ corresponde aos primeiros três “o“ de “foooood“. “o{0,1}“ equivale a “o?“.

[xyz]

Um conjunto de caracteres. Corresponde a qualquer um dos caracteres entre colchetes. Por exemplo, “[abc]“ corresponde ao “a“ de “plain“.

[^xyz]

Um conjunto negativo de caracteres. Corresponde a qualquer caractere não especificado entre colchetes. Por exemplo, “[^abc]“ corresponde ao “p“ de “plain“.

[a-z]

Um intervalo de caracteres. Corresponde a qualquer caractere do intervalo especificado. Por exemplo, “[a-z]“ corresponde a qualquer caractere minúsculo no intervalo de “a“ a “z“.

[^m-z]

Os caracteres de um intervalo negativo. Corresponde a qualquer caractere que não esteja no intervalo especificado. Por exemplo, “[m-z]“ corresponde a qualquer caractere minúsculo que não esteja no intervalo de “m“ a “z“.

\b

Corresponde a um limite de palavra, ou seja, a posição entre uma palavra e um espaço. Por exemplo, “er\b“ corresponde ao “er“ de “never“, mas não ao “er“ de “verb“.

\B

Corresponde a um limite de não-palavra. “ea*r\B“ corresponde ao “ear“ de “never early“.

\d

Corresponde a um caractere numérico. Equivale a [0-9].

\D

Corresponde a um caractere não-numérico. Equivale a [^0-9].

\f

Corresponde ao caractere de avanço de página.

\n

Corresponde ao caractere de nova linha.

\r

Corresponde ao caractere de retorno de carro.

\s

Corresponde a qualquer espaço em branco, incluindo espaço, tabulação, avanço de página, etc. Equivale a “[\f\n\r\t\v]“.

\S

Corresponde a qualquer caractere de espaço que não esteja em branco. Equivale a “[^ \f\n\r\t\v]“.

\t

Corresponde a um caractere de tabulação.

\v

Corresponde a um caractere de barra vertical.

\w

Corresponde a qualquer caractere de palavra, incluindo o sublinhado. Equivale a “[A-Za-z0-9_]“.

\W

Corresponde a qualquer caractere que não seja de palavra. Equivale a “[^A-Za-z0-9_]“.

\num

Corresponde a num, onde num é um número inteiro positivo. Uma referência às correspondências lembradas. Por exemplo, “(.)\1“ corresponde a dois caracteres idênticos consecutivos.

\n

Corresponde a n, onde n é um valor de octal escape. Os valores de octal escape devem conter 1, 2 ou 3 dígitos. Por exemplo, “\11“ e “\011“ correspondem a um caractere de tabulação. “\0011“ equivale a “\001“ & “1“. Os valores de octal escape não devem exceder 256. Caso contrário, apenas os primeiros dois dígitos formarão a expressão. Permite o uso de códigos ASCII em expressões regulares.

\xn

Corresponde a n, onde n é um valor de hexadecimal escape. Os valores de hexadecimal escape devem conter exatamente dois dígitos. Por exemplo, “\x41“ corresponde a “A“. “\x041“ equivale a “\x04“ & “1“. Permite o uso de códigos ASCII em expressões regulares.”

Relatando spams à McAfee

Você pode relatar o spam à McAfee para que ele seja analisado, permitindo criar atualizações de filtros.

1 Clique na guia **Mensagens** e, em seguida, clique na guia **E-mail bloqueado** ou **E-mail aceito**. A página E-mail bloqueado ou E-mail aceito é exibida.

2 Selecione uma mensagem e, em seguida, clique em **Relatar à McAfee**. A caixa de diálogo de confirmação é exibida.

3 Clique em **Sim**. A mensagem é enviada automaticamente à McAfee.

Enviando reclamações manualmente

Envie uma reclamação para impedir que determinado remetente envie mais spams a você. Para obter mais informações sobre como enviar reclamações, consulte *Enviando reclamações e mensagens de erro*na Ajuda online.

1 Clique na guia **Mensagens** e, em seguida, clique na guia **E-mail bloqueado** ou **E-mail aceito**. Uma lista de mensagens é exibida.

2 Selecione uma mensagem para a reclamação e clique em **Enviar uma reclamação**. A caixa de diálogo **Enviar reclamação** é exibida.

3 Selecione para quem você deseja enviar a mensagem.

> **AVISO**
> Na maioria dos casos, você não deve selecionar o **Remetente**. O envio de uma reclamação ao remetente do spam valida seu endereço de e-mail, o que pode aumentar o número de spams que esse remetente enviará a você.

4 Clique em **Avançar** e siga as instruções das caixas de diálogo exibidas.

Enviando mensagens de erro

Para obter mais informações sobre como enviar mensagens de erro, consulte *Enviando reclamações e mensagens de erro*na Ajuda online.

Envie uma mensagem de erro para evitar que um remetente envie mais spams a você.

Enviando uma mensagem de erro manualmente

1. Clique na guia **Mensagens** e, em seguida, clique na guia **E-mail bloqueado** ou **E-mail aceito**. Uma lista de mensagens é exibida.
2. Para enviar uma mensagem de erro sobre uma mensagem de spam específica, selecione a mensagem e clique em **Enviar um erro**. Uma mensagem de erro será enviada para o endereço de resposta da mensagem de spam.

Índice

F

H

I

L

M

N

O

P

Q

R

S

T

U

V

W